

CT-536+ 4-Port Wireless ADSL2+ Router User's Manual



Version A1.7, October 27, 2006



Warning

- Before servicing or disassembling this equipment, always disconnect all power and telephone lines from the device.
- Use an appropriate power supply and a UL Listed telephone line cord. Specification of the power supply is clearly stated in Appendix C - Specifications.

Preface

This manual provides information to network administrators. It covers the installation, operation and applications of the ADSL router.

The reader reading this manual is presumed to have a basic understanding of telecommunications. For product update, new product release, manual revision, software upgrade, technical support, etc., visit Comtrend Corporation at <http://www.comtrend.com>

This document is subject to change without notice.

Copyright

Copyright© 2006 Comtrend Corporation. All rights reserved. The information and messages contained herein are proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written permission by Comtrend Corporation.

Technical support

When you find the product out of service, or that it doesn't work properly, please contact technical support engineer for immediate servicing or email to INT-support@comtrend.com

Table of Contents

CHAPTER 1	INTRODUCTION	5
1.1	FEATURES.....	5
1.2	APPLICATION.....	6
1.3	FRONT PANEL LED INDICATORS.....	7
CHAPTER 2	INSTALLATION	8
2.1	HARDWARE INSTALLATION.....	8
2.2	INSTALLING THE USB DRIVER	9
CHAPTER 3	LOGIN VIA THE WEB BROWSER.....	14
3.1	IP ADDRESS.....	14
3.2	LOGIN PROCEDURE	15
3.3	DEFAULT SETTINGS	16
CHAPTER 4	QUICK SETUP.....	17
4.1	WAN.....	18
4.2	STATISTICS	19
4.2.1	<i>LAN Statistics.....</i>	<i>20</i>
4.2.2	<i>WAN Statistics.....</i>	<i>21</i>
4.2.3	<i>ATM statistics</i>	<i>22</i>
4.2.4	<i>ADSL Statistics</i>	<i>24</i>
4.2.5	<i>Route.....</i>	<i>26</i>
4.2.6	<i>ARP.....</i>	<i>26</i>
4.2.7	<i>DHCP.....</i>	<i>27</i>
CHAPTER 5	QUICK SETUP.....	28
5.1	AUTO QUICK SETUP	29
5.2	MANUAL QUICK SETUP	30
5.2.1	<i>PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).....</i>	<i>32</i>
5.2.2	<i>MAC Encapsulation Routing (MER)</i>	<i>37</i>
5.2.3	<i>IP Over ATM.....</i>	<i>41</i>
5.2.4	<i>Bridging.....</i>	<i>45</i>
CHAPTER 6	ADVANCED SETUP	47
6.1	WAN.....	48
6.2	LAN.....	49
6.3	NAT	50

6.3.1	<i>Virtual Servers</i>	50
6.3.2	<i>Port Triggering</i>	52
6.3.3	<i>DMZ Host</i>	53
6.3.4	<i>ALG</i>	54
6.4	SECURITY	55
6.4.1	<i>IP Filtering</i>	55
6.4.2	<i>Parental Control</i>	58
6.5	QUALITY OF SERVICE	59
6.6	ROUTING	62
6.6.1	<i>Default Gateway</i>	62
6.6.2	<i>Static Route</i>	63
6.6.3	<i>RIP</i>	64
6.7	DNS	65
6.7.1	<i>DNS Server</i>	65
6.7.2	<i>Dynamic DNS</i>	66
6.8	DSL	68
6.9	PORT MAPPING	69
CHAPTER 7 WIRELESS		71
7.1	WIRELESS BASIC SCREEN	71
7.1.1	<i>Security</i>	73
7.1.2	<i>MAC Filter</i>	76
7.1.3	<i>Wireless Bridge</i>	78
7.1.4	<i>Advanced</i>	79
7.1.5	<i>Station Info</i>	82
CHAPTER 8 DIAGNOSTICS		83
CHAPTER 9 MANAGEMENT		85
9.1	SETTINGS	85
9.1.1	<i>Configuration Backup</i>	86
9.1.2	<i>Tools – Update Settings</i>	87
9.1.3	<i>Restore Default</i>	88
9.2	SYSTEM LOG	90
9.3	SNMP AGENT	92
9.4	INTERNET TIME	93
9.5	ACCESS CONTROL	94
9.5.1	<i>Services</i>	95
9.5.2	<i>Access IP Addresses</i>	96
9.5.3	<i>Passwords</i>	97

9.6	UPDATE SOFTWARE.....	98
9.7	SAVE AND REBOOT	99
APPENDIX A: FIREWALL		100
APPENDIX B: PIN ASSIGNMENTS.....		106
APPENDIX C: SPECIFICATIONS.....		107
APPENDIX D: SSH CLIENT		109

Chapter 1 Introduction

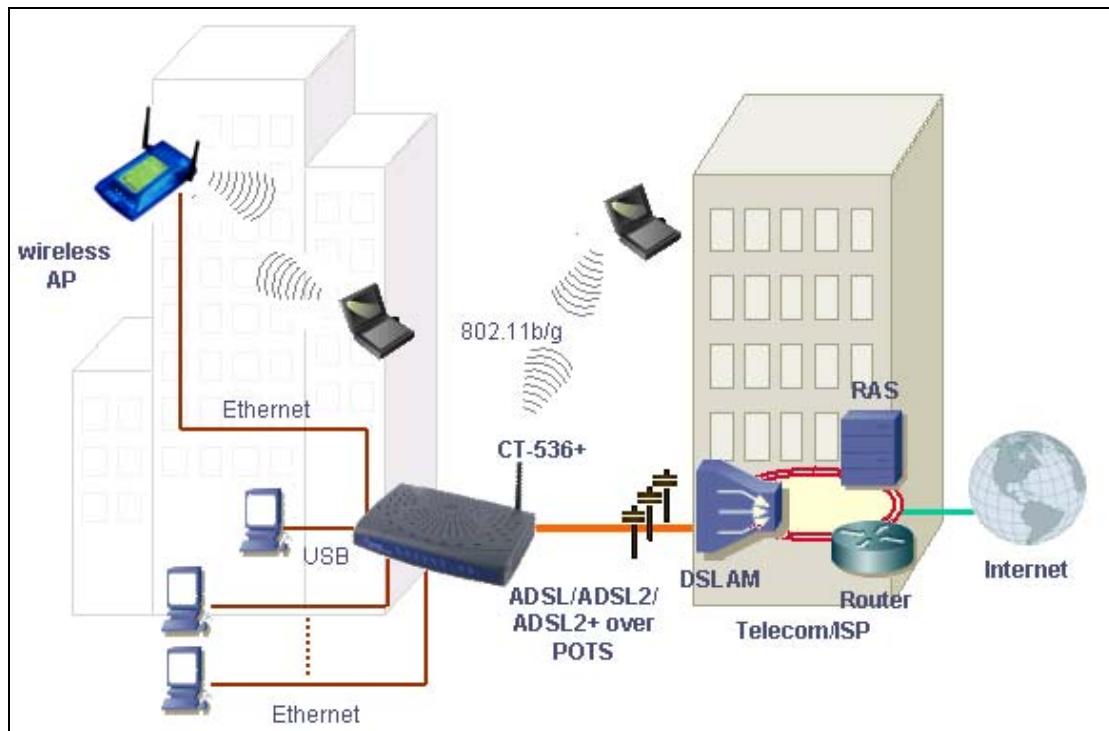
The CT-536+ is an 802.11g (54Mbps) wireless and wired Local Area Network (WLAN) ADSL router. Four 10/100 Base-T Ethernet ports provide wired LAN connectivity with an integrated 802.11g WiFi WLAN Access Point (AP) for wireless connectivity. The CT-536+ ADSL router provides state of the art security features such as WPA data encryption Firewall, VPN pass through. The CT-536+ is designed for both residential and business applications that require wireless and wired connectivity to an ADSL broadband network. The CT-536+ supports up to 8 contiguous virtual connections allowing for multiple simultaneous Internet connections.

1.1 Features

- UPnP
- Integrated 802.11g AP
- Backward compatible with 802.11b
- RADIUS client
- WPA and 802.1x
- Up to 125Mbps for wireless (Afterburner mode)
- Wireless QoS (WMM)
- IP/MAC address filtering
- Static route/RIP/RIP v2 routing functions
- Dynamic IP assignment
- IP/Bridge QoS
- NAT/PAT
- IGMP Proxy
- DHCP Server/Relay/Client
- DNS Proxy
- Auto PVC configuration
- Per-VC packet level QoS
- Up to 16 VCs
- Embedded SNMP agent
- Web-based management
- Remote configuration and upgrade
- Configuration backup and restoration
- FTP server
- TFTP server
- IGMP Snooping
- 802.1q/802.1p

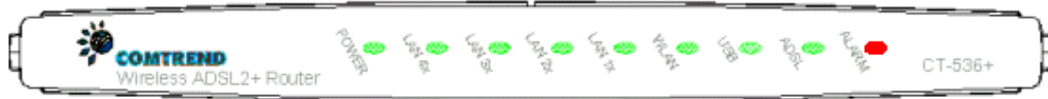
1.2 Application

The following diagram depicts the application of the CT-536+ on a wireless network.



1.3 Front Panel LED Indicators

The front panel LEDs are shown in the picture below, followed by an explanation in the table below.

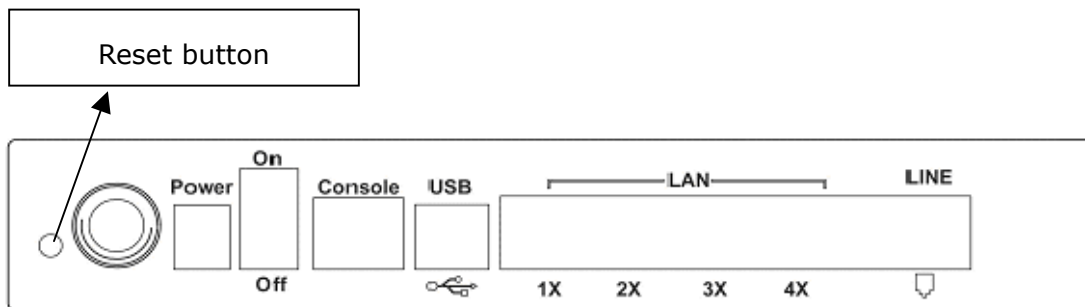


LED	Color	Mode	Function
POWER	Green	On	The router is powered up.
		Off	The router is powered down.
LAN 1x~4x	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
	Green	Blink	Data transmitting or receiving over LAN.
WLAN	Green	On	The wireless module is ready and idle.
		Off	The wireless module is not installed.
	Green	Blink	Data transmitting or receiving over WLAN.
USB	Green	On	A USB link is established.
		Off	A USB link is not established.
	Green	Blink	Data transmitting or receiving over USB.
ADSL	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.
	Green	Blink	The ADSL link is training or some traffic is passing through ADSL.
ALARM	Red	On	The ADSL link is terminated.
		Off	Normal operating status.

Chapter 2 Installation

2.1 Hardware Installation

In the rear panel, there is a reset button. To load the factory default settings, hold the reset button down for at least 5 seconds.



Follow the instructions below to complete the hardware connections.

Connection to LINE port

If you wish to connect both the router and a telephone, connect the LINE port to a POTS splitter with a RJ11 connection cable.

Connection to LAN port

To connect to a hub or PC, use a RJ45 cable. You can connect the router to up to four LAN devices. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

Connection to Console port

(Optional) In order to manage your device through the console port you will need to use a straight-through cable with an **RJ-45 connector** to attach to the modem, and a **female RS-232 connector** to connect to the serial port on a PC. The PC must be equipped with a VT-100 emulation program, such as HyperTerminal 5 or Telix. The Console session parameters are Baud rate 115200 bps; Data bits 8; Parity none Stop bit 1; Flow control none.

Please see **Appendix B** for the console cable Pin Assignment.

Connection to Power

Connect the **Power** jack to the shipped power cord. Attach the power adapter to the wall outlet or other AC source.

After all connections have been made, turn the power-switch to the on position.

After power on, the router performs a self-test. Wait for a few seconds until the test is finished, then the router will be ready to operate.

Caution 1: If the router fails to power up, or it malfunctions, first verify that the power supply is connected correctly. Then power it on again. If the problem persists, contact our technical support engineers.

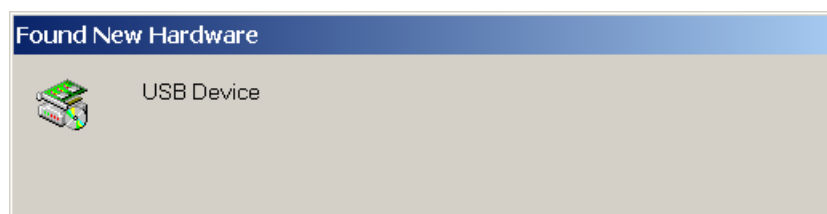
Caution 2: Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from the wall outlet.

2.2 Installing the USB Driver

Before you connect your router's USB cable to your PC, you must load the ADSL USB drivers. The USB driver supports Windows 98, ME, 2000, and XP.

To connect the router to a PC using the USB interface, you need to use a standard USB cable and install the USB interface software. Follow the steps below:

STEP 1: Connect the USB router to the PC by plugging the flat connector of a standard USB cable into your PC, and plugging the square connector into the router. The screen will display as below:

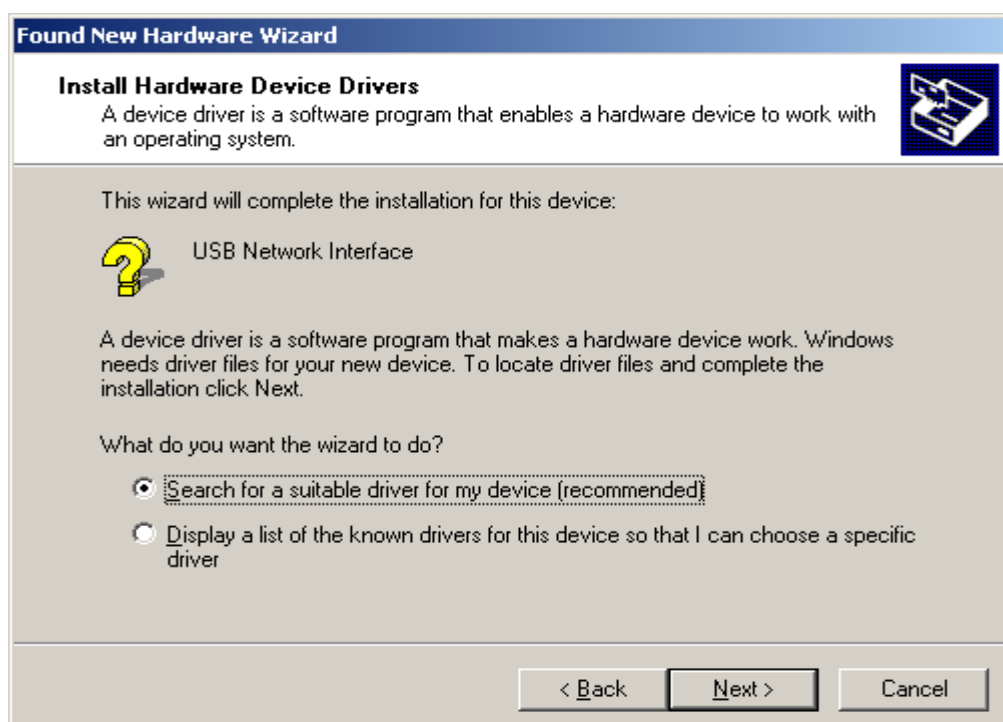


STEP 2: When the screen displays as below, click the **Next** button.

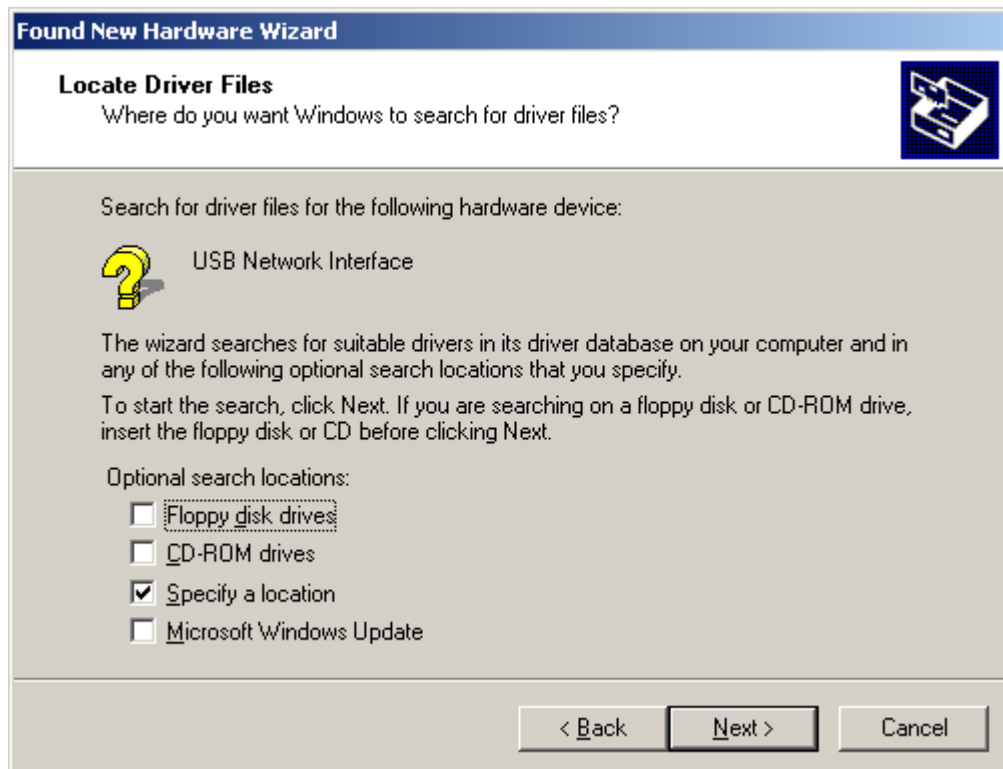


Note: This screen won't be displayed if the USB Driver has been previously un/installed.

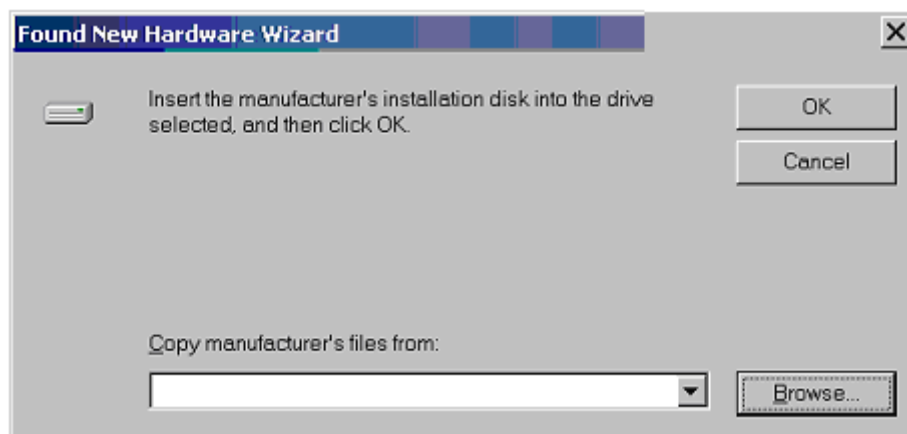
STEP 3: When the screen displays as below, select **Search for a suitable driver** and click the **Next** button.



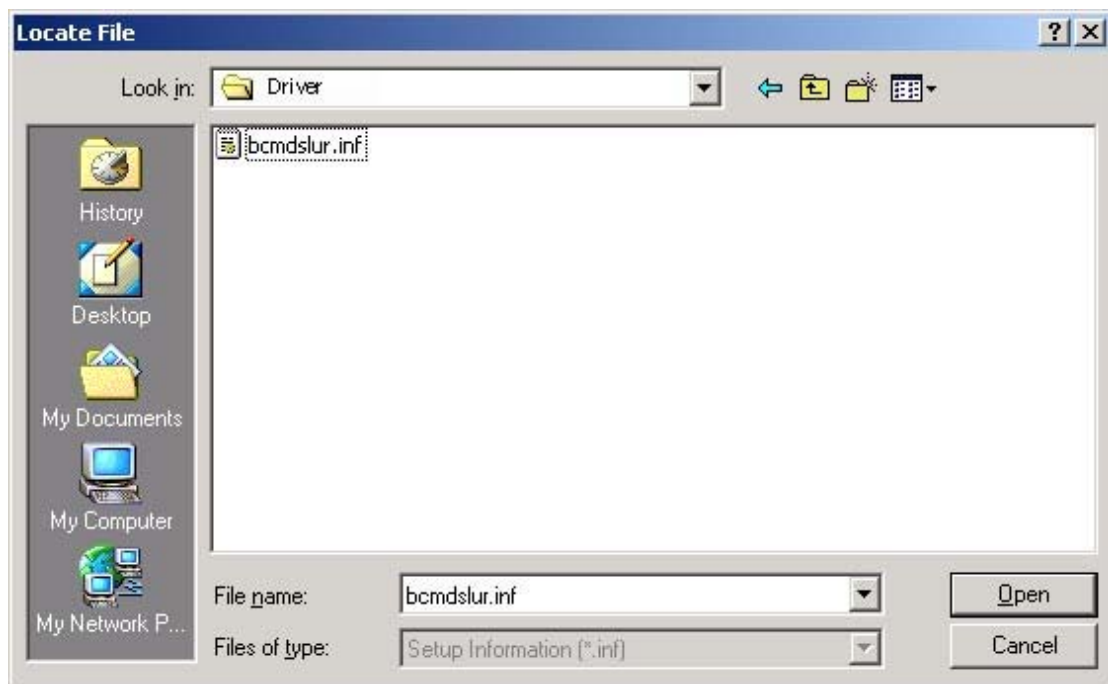
STEP 4: Select Specify a location and click the Next button. If you are installing the software from a disk, insert the disk.



STEP 5: Select the location of the file using the **Browse** button. Normally, the file is on the CD-ROM shipped with the device.



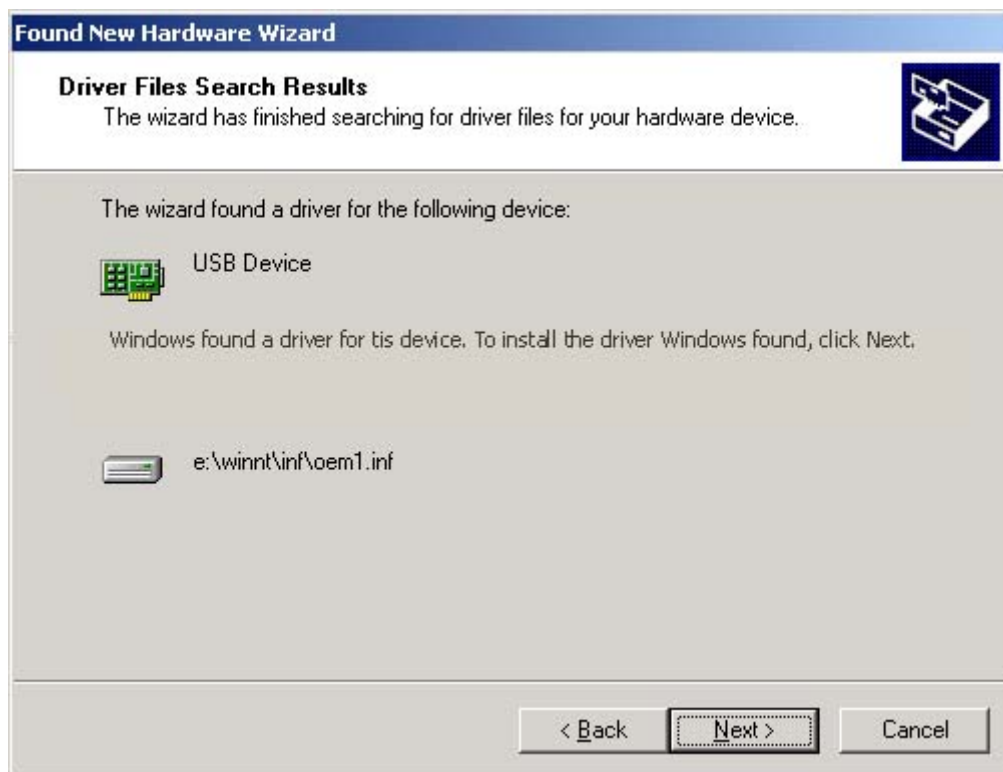
STEP 6: Locate the file, and click the **Open** button.



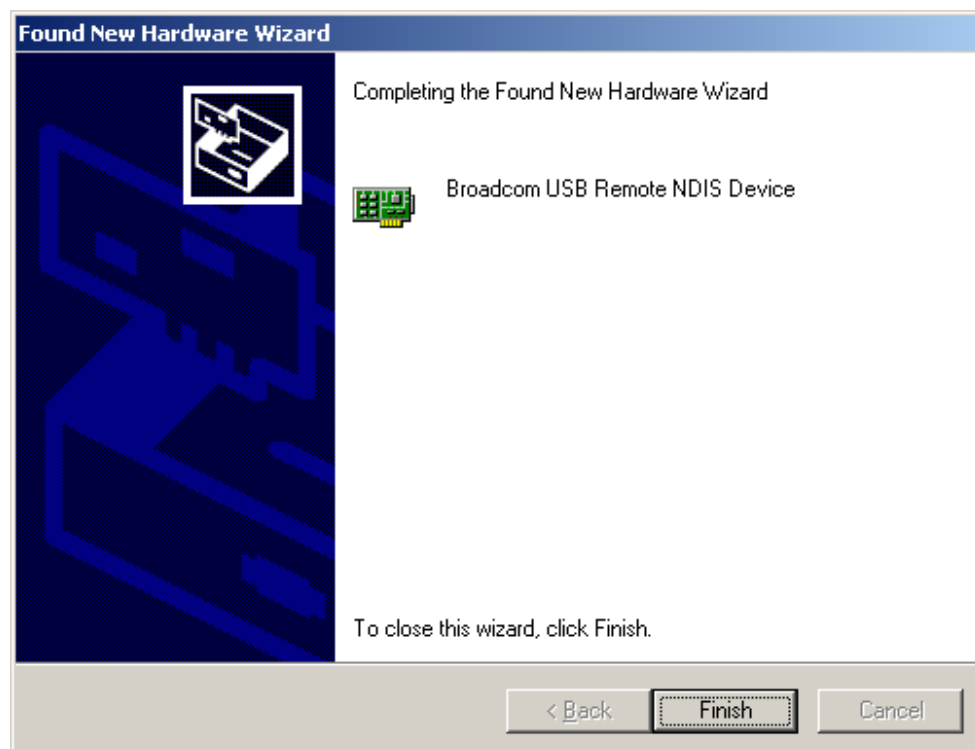
STEP 7: When the screen displays as below, click the **OK** button.



STEP 8: When the screen below displays, click the **NEXT** button.



STEP 9: Click the **Finish** button, when the screen displays as below.



STEP 10: Installation is complete.

Chapter 3 Login via the Web Browser

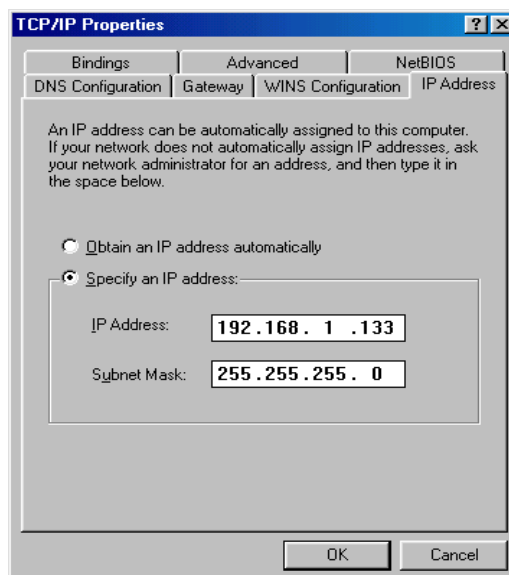
This section describes how to manage the router via a Web browser via the remote end. You can use a web browser such as Microsoft Internet Explorer, or Netscape Navigator. (The Web page is best viewed with Microsoft Internet Explorer 5.0 and later): A unique default user account is assigned with user name **root** and password **12345**. The user can change the default password later when logged in to the device.

3.1 IP Address

The default IP address of the CT-536+ (LAN port) is 192.168.1.1. To configure the CT-536+ for the first time, the configuration PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x.

STEP 1: Right click on the Local Area Connection under the Network and Dial-Up connection window and select Properties.

STEP 2: Enter the TCP/IP screen and change the IP address to the domain of 192.168.1.x/24.



STEP 3: Click **OK** to submit the settings.


STEP 4: Start your Internet browser and type the IP address for the router (192.168.1.1) in the Web address bar.

3.2 Login Procedure

Perform the following steps to bring up the Web user interface and configure the CT-536+. To log on to the system from the Web browser, follow the steps below:

STEP 1: Start your Internet browser. Type the IP address for the router in the Web address field. For example, if the IP address is 192.168.1.1, type **http://192.168.1.1**

STEP 2: You will be prompted to enter your user name and password. Type **root** in the user name and **12345** in the password field, and click **OK**. These values can be changed later in the Web User Interface by selecting the **Management** link.



STEP 3: After successfully logging in, you will reach the Quick Setup screen.



3.3 Default Settings

During power on initialization, the CT-536+ initializes all configuration attributes to default values. It will then read the configuration profile from the Permanent Storage section on the flash memory. The default attributes are overridden when identical attributes with different values are configured. The configuration profile in Permanent Storage can be created via the Web user interface, the console, or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds, or by clicking the Restore Default Configuration option in the Restore Settings screen.

The following default settings are present when setting up the router for the first time.

- LAN port IP address: 192.168.1.1
- Console port: 115200 bps
- Local administrator account name: root
- Local administrator account password: 12345
- Local non- administrator account name: user
- Local non- administrator account password: user
- Remote WAN access: disabled
- Remote WAN access account name: root
- Remote WAN access account password: 12345
- NAT and firewall: disabled
- DHCP server on LAN interface: enable
- WAN IP address: none

Chapter 4 Quick Setup

After login, the **Quick Setup** screen appears as shown.



COMTREND ADSL Router

Quick Setup

This Quick Setup will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration

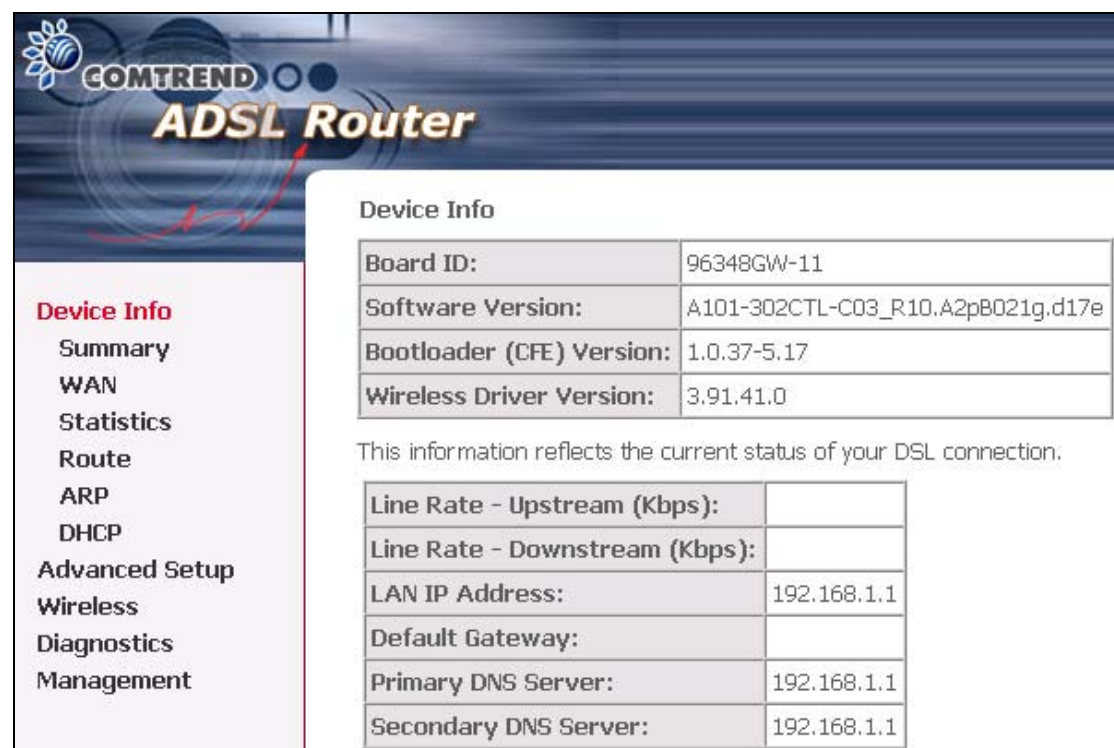
Select the check box below to enable DSL Auto-connect process.

☒ DSL Auto-connect

Next

Note: The selections available on the left side of menu are based upon the configured connection.

If you configure a PVC and Click Save/Reboot, the Device Info screen will be displayed.



COMTREND ADSL Router

Device Info

Board ID:	96348GW-11
Software Version:	A101-302CTL-C03_R10.A2pB021g.d17e
Bootloader (CFE) Version:	1.0.37-5.17
Wireless Driver Version:	3.91.41.0

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1

4.1 WAN

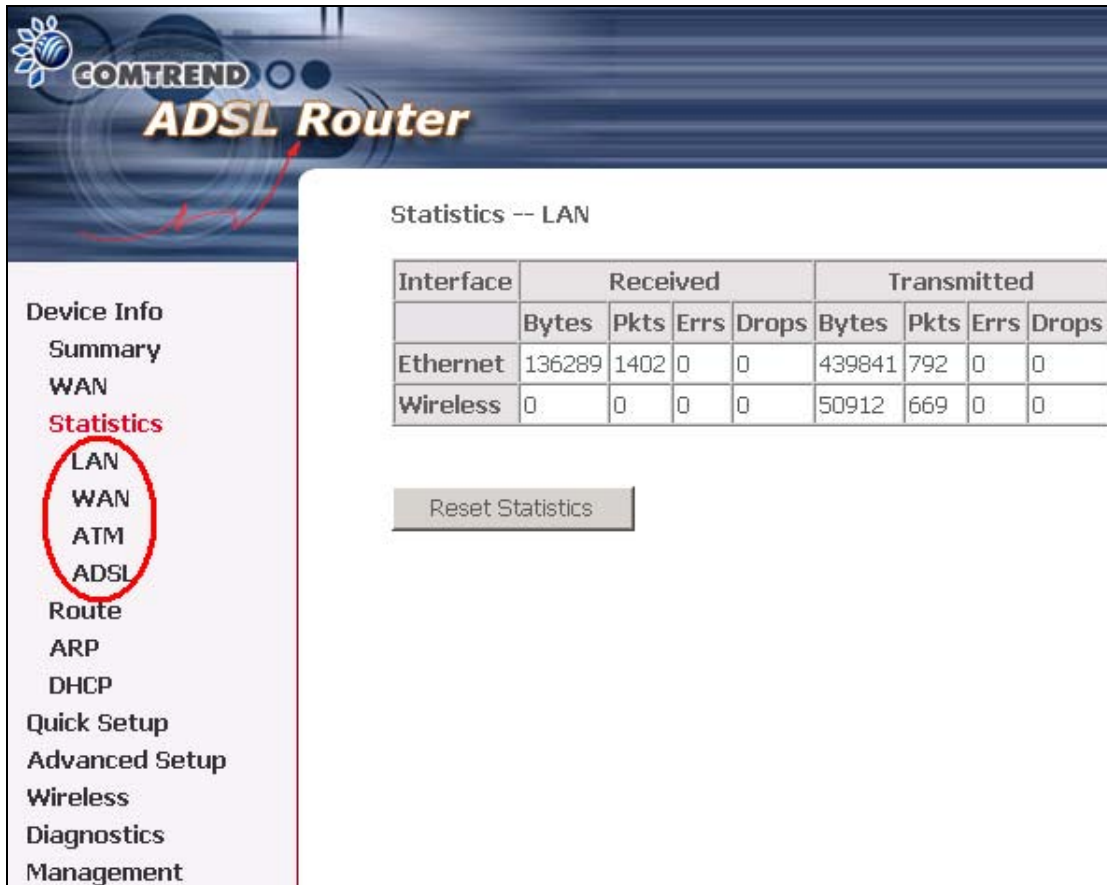
Click **Device Info** on the menu bar to display the WAN option. Then, click **WAN** on the Device Info menu bar to display the configured PVC(s) and the status.



VPI/VCI	Shows the values of the ATM VPI/VCI
Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
IGMP	Shows the state of the IGMP function
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IP Address	Shows IP address for WAN interface

4.2 Statistics

Selection of the Statistics screen provides statistics for the Network Interface of LAN, WAN, ATM and ADSL. All statistics screens are updated every 15 seconds.



COMTREND
ADSL Router

Device Info
Summary
WAN
Statistics
 LAN
 WAN
 ATM
 ADSL
Route
ARP
DHCP
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

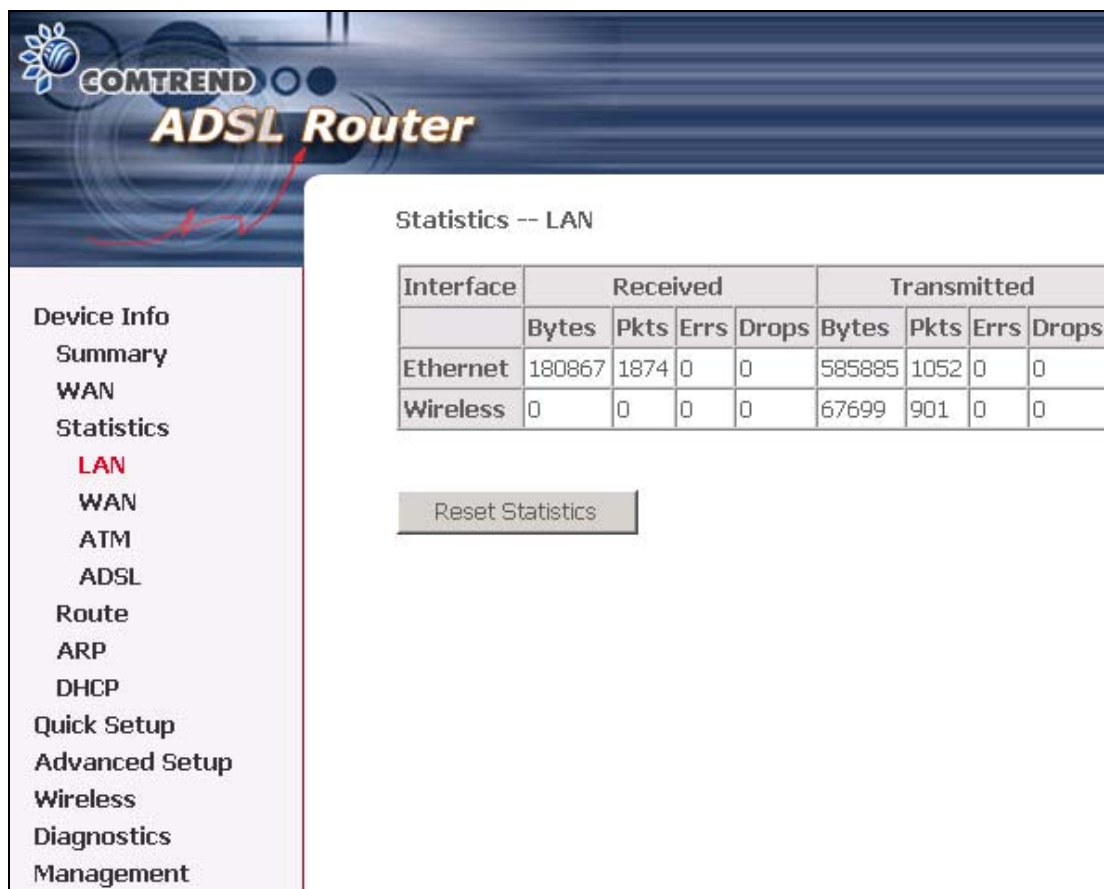
Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	136289	1402	0	0	439841	792	0	0
Wireless	0	0	0	0	50912	669	0	0

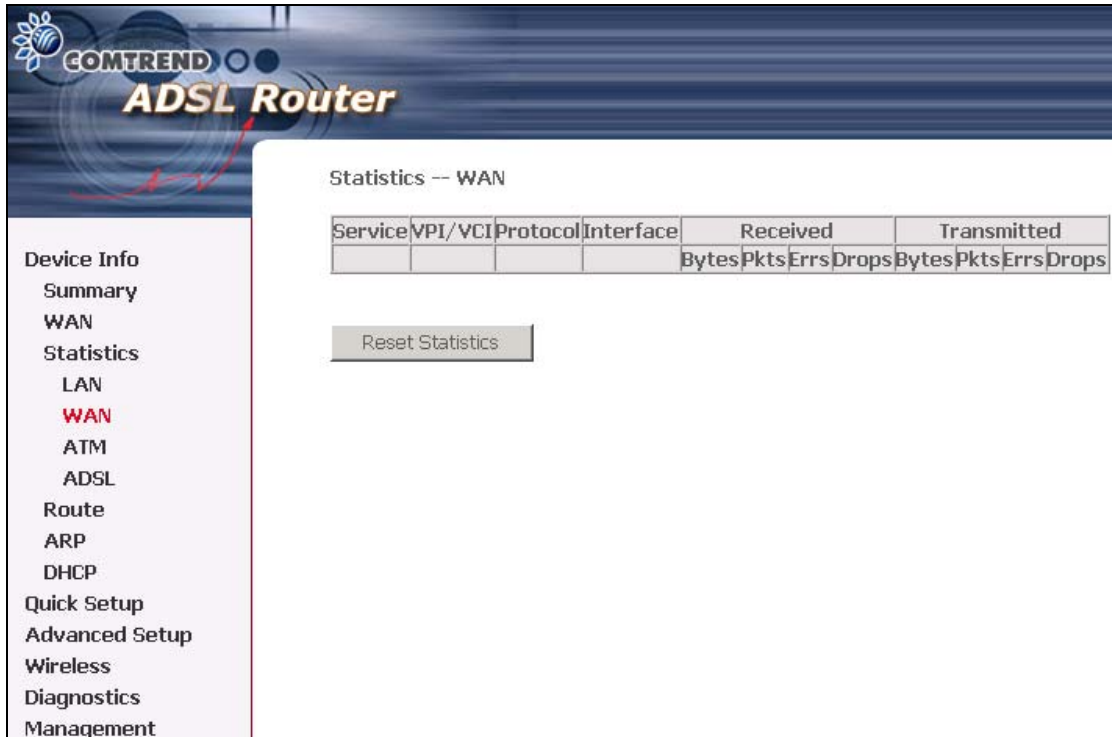
Reset Statistics

4.2.1 LAN Statistics

The Network Statistics screen shows interface statistics for ATM AAL5 interface, Ethernet and USB interfaces. (The Network Statistics screen shows interface statistics for LAN of Ethernet and USB interfaces. This provides byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)



4.2.2 WAN Statistics

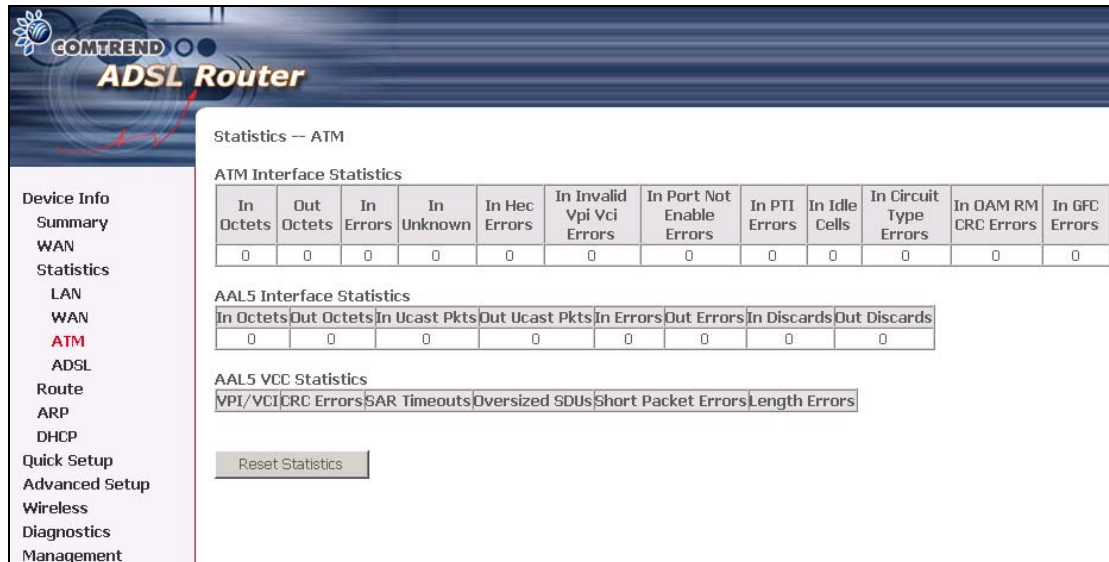


The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with the following items: Device Info, Summary, WAN, Statistics, LAN, WAN (highlighted in red), ATM, ADSL, Route, ARP, DHCP, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Statistics -- WAN". It contains a table with the following columns: Service, VPI/VCI, Protocol, Interface, Received (sub-columns: Bytes, Pkts, Errs, Drops), and Transmitted (sub-columns: Bytes, Pkts, Errs, Drops). Below the table is a "Reset Statistics" button.

Service	Shows the service type
VPI/VCI	Shows the values of the ATM VPI/VCI
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
Interface	Shows connection interfaces
Received/Transmitted	<ul style="list-style-type: none"> - Bytes Rx/TX (receive/transmit) packet in Bytes - Pkts Rx/TX (receive/transmit) packets - Errs Rx/TX (receive/transmit) the packets which are errors, - Drops Rx/TX (receive/transmit) the packets which are dropped

4.2.3 ATM statistics

The following figure shows the ATM statistics screen.



ATM Interface Statistics

Field	Description
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEC error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enabled Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In Oam RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

ATM AAL5 Layer Statistics over ADSL interface

Field	Description
In Octets	Number of received AAL5/AAL0 CPCS PDU octets
Out Octets	Number of received AAL5/AAL0 CPCS PDUs octets transmitted
In Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer for transmission
Out Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs received from a higher layer for transmission
In Errors	Number of received AAL5/AAL0 CPCS PDUs received in error. The types of errors counted include CRC-32 errors.
Out Errors	Number of received AAL5/AAL0 CPCS PDUs that could be transmitted due to errors.
In Discards	Number of received AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition.
Out Discards	This field is not currently used

ATM AAL5 LAYER STATISTICS FOR EACH VCC OVER ADSL INTERFACE

Field	Description
CRC Errors	Number of PDUs received with CRC-32 errors
SAR TimeOuts	Number of partially re-assembled PDUs which were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value.
Over Sized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packets Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

4.2.4 ADSL Statistics

The following figure shows the ADSL Network Statistics screen. Within the ADSL Statistics window, a bit Error Rate Test can be started using the ADSL BER Test button. The Reset button resets the statistics.

COMTREND ADSL Router

Statistics -- ADSL

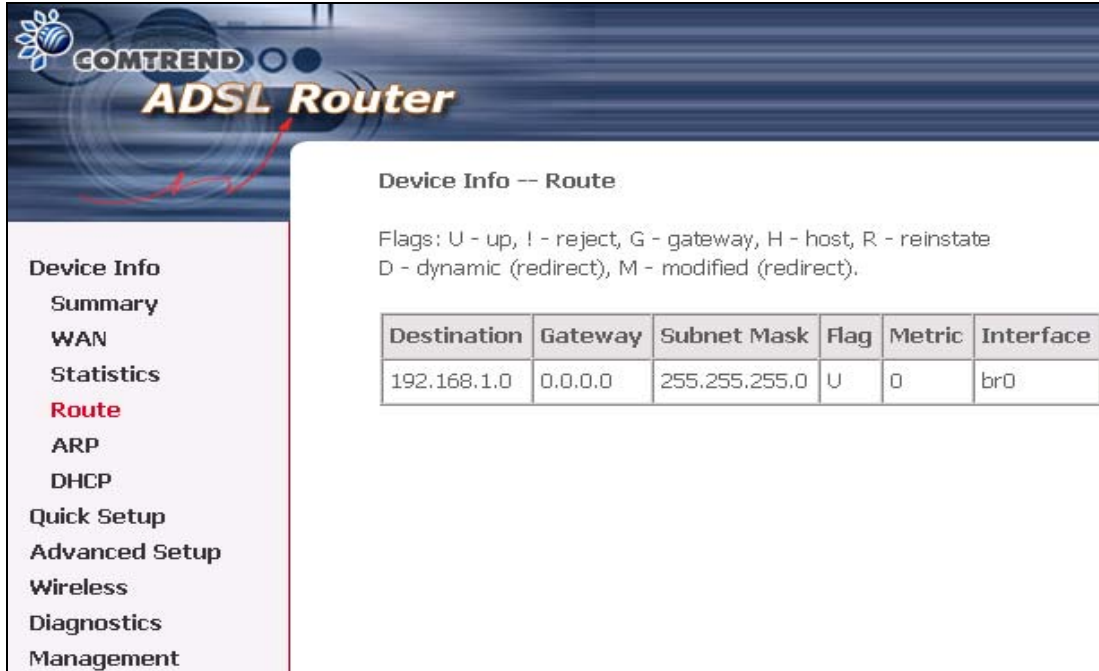
Mode:		
Type:		
Line Coding:		
Status:		Link Down
Link Power State:		LO
	Downstream	Upstream
SNR Margin (dB):		
Attenuation (dB):		
Output Power (dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		N/A
Data Cells:		N/A
Bit Errors:		N/A
Total ES:		
Total SES:		
Total UAS:		

ADSL BER Test Reset Statistics

Field	Description
Mode	Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2
Type	Channel type Interleave or Fast
Line Coding	Trellis On/Off
Status	Lists the status of the DSL link
Link Power State	Link output power state.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

4.2.5 Route

Choose **Route** to display the routes that the route information has learned.




The screenshot shows the COMTREND ADSL Router web interface. The left sidebar contains a menu with the following items: Device Info, Summary, WAN, Statistics, **Route** (highlighted in red), ARP, DHCP, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Device Info -- Route". It includes a legend: "Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect)". Below the legend is a table with the following data:

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	br0

4.2.6 ARP

Click **ARP** to display the ARP information.

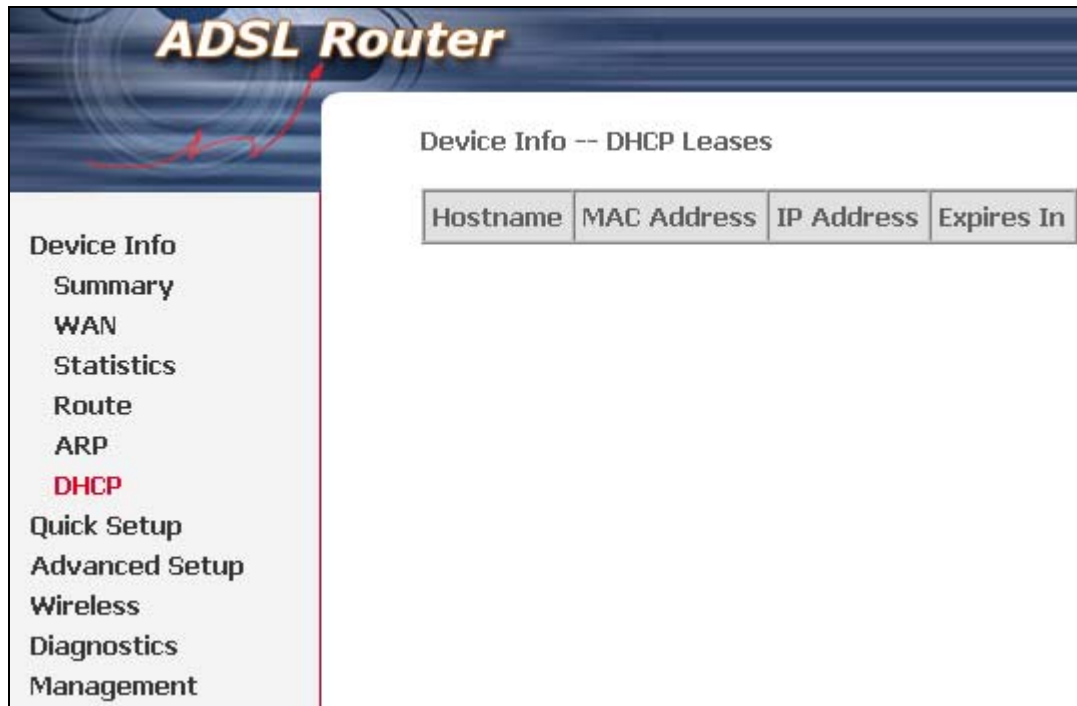


The screenshot shows the COMTREND ADSL Router web interface. The left sidebar contains a menu with the following items: Device Info, Summary, WAN, Statistics, Route, **ARP** (highlighted in red), DHCP, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Device Info -- ARP". It includes a table with the following data:

IP address	Flags	HW Address	Device
192.168.1.133	Complete	00:05:5D:0C:56:E1	br0

4.2.7 DHCP

Click **DHCP** to display the DHCP information.



The screenshot displays the web interface of an ADSL Router. The top header features the text "ADSL Router" in a stylized font. On the left side, there is a vertical navigation menu with the following items: "Device Info", "Summary", "WAN", "Statistics", "Route", "ARP", "DHCP" (highlighted in red), "Quick Setup", "Advanced Setup", "Wireless", "Diagnostics", and "Management". The main content area is titled "Device Info -- DHCP Leases". Below this title is a table with four columns: "Hostname", "MAC Address", "IP Address", and "Expires In". The table is currently empty, showing only the header row.

Hostname	MAC Address	IP Address	Expires In
----------	-------------	------------	------------

Chapter 5 Quick Setup

The Quick Setup allows the user to configure the ADSL router for DSL connectivity and Internet access. It also guides the user through the WAN network setup first and then the LAN interface setup. You can either manually customize the router or follow the online instruction to set up the router.

The CT-536+ ADSL router supports the following five network operating modes over an ATM PVC WAN interface.

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration on the Central Office side and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the CT-536+ is to run the PPPoE client. The CT-536+ can support both cases simultaneously.
- If some or none of the LAN-side devices do not run PPPoE client, then select PPPoE. If every LAN-side device is running a PPPoE client, then select Bridge. In PPPoE mode, CT-536+ also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client for non-PPPoE LAN devices. NAT and firewall are always enabled when PPPoE mode is selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAT and firewall are always disabled when Bridge mode is selected.
- Depending on the network operating mode, and whether NAT and firewall are enabled or disabled, the main panel will display or hide the NAT/Firewall menu. For instance, at initial setup, the default network operating mode is Bridge. The main panel will not show the NAT and Firewall menu.

Note: Up to eight PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you need to navigate all the Quick Setup pages until the last summary page, then click on the Finish button and reboot the system.

5.1 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL router will automatically detect the PVC. You only need to follow the online instructions that you are prompted.

1. Select **Quick Setup** to display the DSL Quick Setup screen.



2. Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some processes like PVC index, or encapsulation.
3. After the settings are complete, you can use the ADSL service.

5.2 Manual Quick Setup

STEP 1: Click **Quick Setup** and un-tick the **DSL Auto-connect** checkbox to enable manual configuration of the connection type.



COMTREND
ADSL Router

Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

Quick Setup

This Quick Setup will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration

Select the check box below to enable DSL Auto-connect process.

☒ DSL Auto-connect

Un-tick this checkbox to enable manual setup and display the following screen.

The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.

VPI: [0-255]

VCI: [32-65535]

Enable Quality Of Service

Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service ☐

Next

STEP 2: Enter the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). Select Enable Quality Of Service if required. Click **Next**.

STEP 3: STEP 3: Then, choose the Encapsulation mode. Select **Enable 802.1q** (by ticking the box) if required, and input a number for the VLAN ID. Click Next.

The screenshot displays the COMTREND ADSL Router configuration web interface. On the left is a sidebar menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled 'Connection Type' and includes a note: 'Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.' Below this, there are five radio button options: 'PPP over ATM (PPPoA)', 'PPP over Ethernet (PPPoE)', 'MAC Encapsulation Routing (MER)', 'IP over ATM (IPoA)', and 'Bridging'. The 'Bridging' option is selected. Under the 'Encapsulation Mode' section, a dropdown menu is set to 'LLC/SNAP-BRIDGING'. Below that, the 'Enable 802.1q' checkbox is currently unchecked. A red arrow points from this checkbox to a second, zoomed-in screenshot below. This second screenshot shows the 'Enable 802.1q' checkbox checked and a 'VLAN ID[0-4095]:' text box next to it. Both screenshots have 'Back' and 'Next' buttons at the bottom right.

STEP 4: Click **Next** to display the following screen. Choosing different connection types pops up different settings requests. Enter appropriate settings that are requested by your service provider. The following descriptions state each connection type setup separately.

5.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

1. Select the **PPP over ATM (PPPoA)** or **PPP over Ethernet (PPPoE)** radio button and click **Next**. The following screen appears:

The screenshot shows the 'PPP Username and Password' configuration page of a COMTREND ADSL Router. The page has a blue header with the COMTREND logo and 'ADSL Router' text. On the left is a navigation menu with links: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled 'PPP Username and Password' and includes a descriptive paragraph: 'PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.' Below this are input fields for 'PPP Username:', 'PPP Password:', and 'PPPoE Service Name:'. The 'Authentication Method:' is set to 'AUTO' via a dropdown menu. There are five checkboxes: 'Dial on demand (with idle timeout timer)', 'PPP IP extension', 'Enable NAT', 'Use Static IP Address', and 'Fixed MTU' (which is checked). Below the 'Fixed MTU' checkbox is an 'MTU:' field with the value '1492'. At the bottom right are 'Back' and 'Next' buttons.

PPP USERNAME/PPP PASSWORD

The PPP Username and the PPP password requirement are dependent on the particular requirements of the ISP or the ADSL service provider. The WEB user interface allows a maximum of 256 characters in the PPP user name and a maximum of 32 characters in PPP password.

Encapsulation Mode

Choosing different connection types provides different encapsulation modes.

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP BRIDGING, VC/MUX
- MER- LLC/SNAP-BRIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- Bridging- LLC/SNAP-BRIDGING, VC/MUX

Disconnect if no activity

The CT-536+ can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes.

<input checked="checked" type="checkbox"/> Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]: <input type="text"/>

PPP IP Extension

The PPP IP Extension is a special feature deployed by some service providers.

Unless your service provider specially requires this setup, do not select it.

The PPP IP Extension supports the following conditions:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC's LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the ADSL router has a single IP address to assign to a LAN device.
- NAPT and firewall are disabled when this option is selected.
- The ADSL router becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The ADSL router extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The ADSL router bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the router's LAN IP address.

2. Click **Next** to display the following screen.

Enable IGMP Multicast checkbox: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service checkbox: Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is user-defined.

Enable NAT checkbox: If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel. The default setting for PPPoE/PPPoA is disabled.

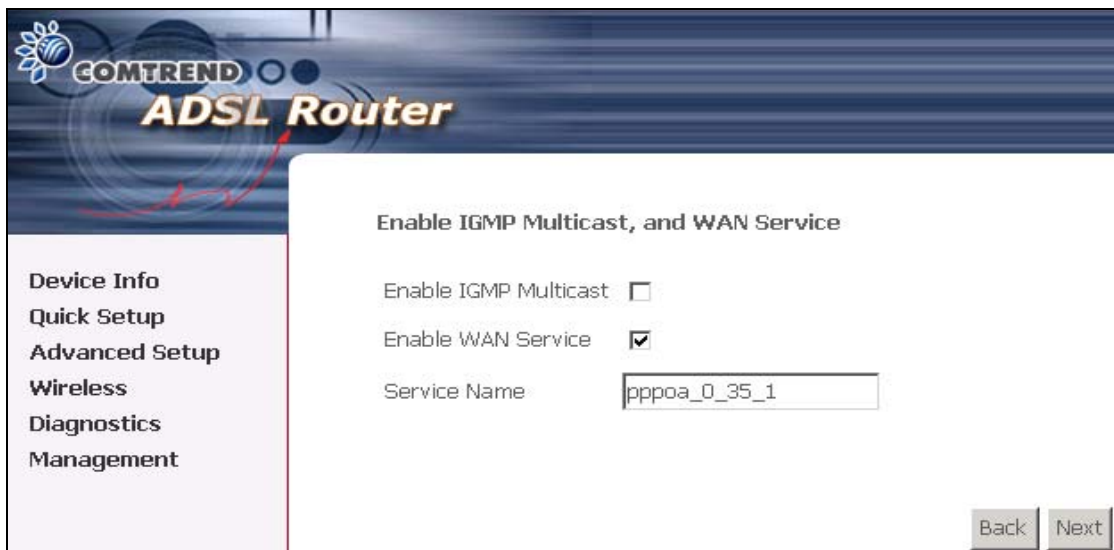
Use Static IP Address

Unless your service provider specially requires this setup, do not select it.

If selected, enter your static IP address.


MTU

This option allows us to change the MTU size for WAN interface, PPPoE and PPPoA. The default value is 1492 for PPPoE and 1500 for PPPoA.



3. After entering your settings, select **Next**. The following screen appears. This page allows the user to configure the LAN interface IP address, subnet mask and DHCP server. If the user would like this ADSL router to assign dynamic IP address, DNS server and default gateways to other LAN devices, select the button **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP leased time.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address.



Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

☐ Disable DHCP Server
☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

☐ Enable DHCP Server Relay
 DHCP Server IP Address:

☐ Configure the second IP Address and Subnet Mask for LAN interface

Back Next

4. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.



Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

Wireless -- Setup

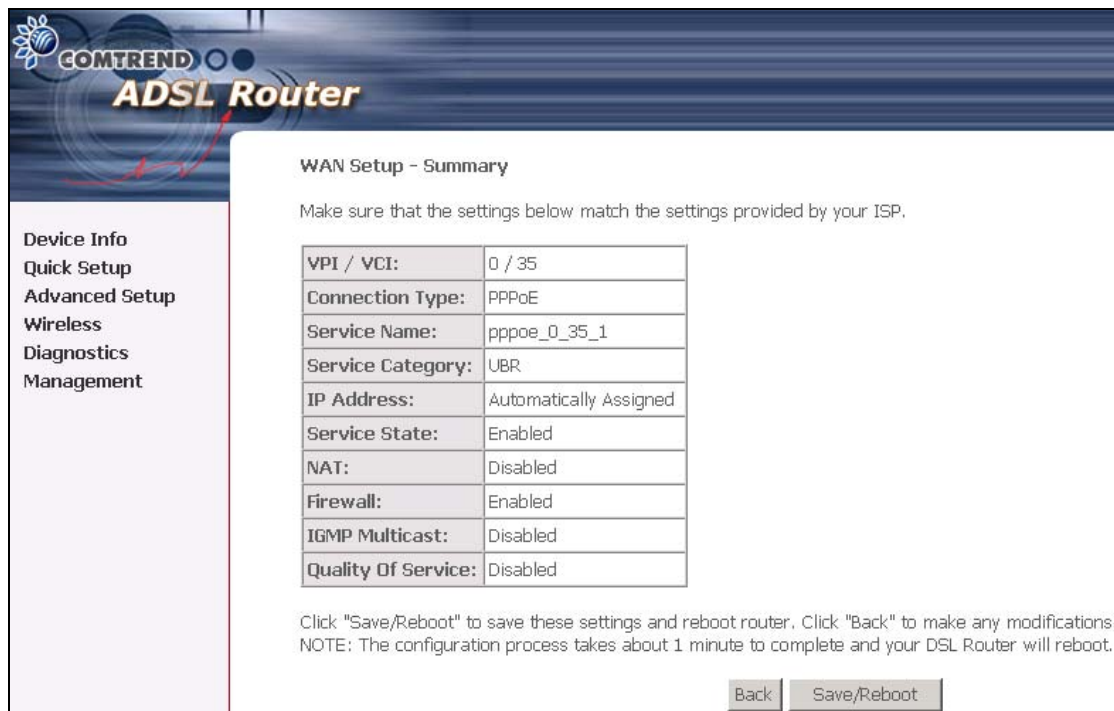
Enable Wireless ☒

Enter the wireless network name (also known as SSID).

SSID:

Back Next

5. Click **Next** to display the WAN Setup-Summary screen that presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.



The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main area is titled 'WAN Setup - Summary' and includes a warning to match ISP settings. A table lists configuration parameters: VPI / VCI (0 / 35), Connection Type (PPPoE), Service Name (pppoe_0_35_1), Service Category (UBR), IP Address (Automatically Assigned), Service State (Enabled), NAT (Disabled), Firewall (Enabled), IGMP Multicast (Disabled), and Quality Of Service (Disabled). At the bottom are 'Back' and 'Save/Reboot' buttons. A note states that saving and rebooting takes about 1 minute.

COMTREND ADSL Router

Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
 NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

6. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-536+ is ready for operation and the LEDs display as described in the LED description tables.

5.2.2 MAC Encapsulation Routing (MER)

To configure MER, do the following.

1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index provided by the ISP and click **Next**.
3. Select the MAC Encapsulation Routing (MER) radio button, and click **Next**. The following screen appears.

The screenshot shows the WAN IP Settings page of a COMTREND ADSL Router. The page has a blue header with the COMTREND logo and 'ADSL Router' text. On the left is a navigation menu with 'Device Info', 'Quick Setup', 'Advanced Setup', 'Wireless', 'Diagnostics', and 'Management'. The main content area is titled 'WAN IP Settings' and contains instructions: 'Enter information provided to you by your ISP to configure the WAN IP settings. Notice: DHCP can be enabled for PVC in MER mode if "Obtain an IP address automatically" is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection. If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.' There are three main sections: 1. IP Addressing: 'Obtain an IP address automatically' (selected) or 'Use the following IP address:' with fields for 'WAN IP Address:' and 'WAN Subnet Mask:'. 2. Default Gateway: 'Obtain default gateway automatically' (selected) or 'Use the following default gateway:' with sub-options 'Use IP Address:' (checkbox) and 'Use WAN Interface:' (checkbox, dropdown menu showing 'mer_0_35/nas_0_35'). 3. DNS Settings: 'Obtain DNS server addresses automatically' (selected) or 'Use the following DNS server addresses:' with fields for 'Primary DNS server:' and 'Secondary DNS server:'. At the bottom right are 'Back' and 'Next' buttons.

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP can be enabled for PVC in MER mode if **Obtain an IP address automatically** is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.

If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

The ISP should provide the values that must be entered in the entry fields.

4. Click **Next** to display the following screen.

The screenshot shows the 'Network Address Translation Settings' page of a COMTREND ADSL Router. The left sidebar contains a menu with 'Device Info', 'Quick Setup', 'Advanced Setup', 'Wireless', 'Diagnostics', and 'Management'. The main content area has a title 'Network Address Translation Settings' and a description: 'Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN)'. Below this are three checkboxes: 'Enable NAT' (unchecked), 'Enable Firewall' (unchecked), and 'Enable IGMP Multicast, and WAN Service'. Under the third checkbox, there are two more checkboxes: 'Enable IGMP Multicast' (unchecked) and 'Enable WAN Service' (checked). A 'Service Name' field contains the text 'mer_0_35'. At the bottom right are 'Back' and 'Next' buttons.

Enable NAT checkbox: If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel. The default setting for MER is disabled.

Enable Firewall checkbox: If the firewall checkbox is selected, the Security submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main panel.

Enable IGMP Multicast: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service: Tick the checkbox to enable the WAN service. If this item is not selected, you will not be able to use the WAN service.

Service Name: This is User-defined.

5. Upon completion, click **Next**. The following screen appears.

COMTREND ADSL Router

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

☐ Enable DHCP Server Relay

DHCP Server IP Address:

☐ Configure the second IP Address and Subnet Mask for LAN interface

The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

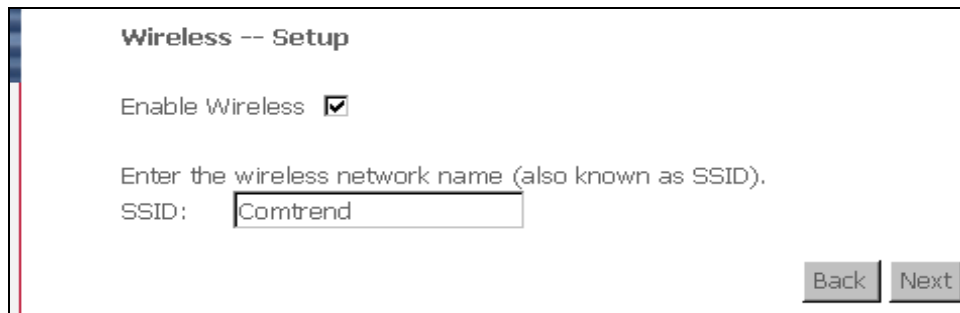
Note that the router's default IP address is 192.168.1.1 and the default private address range provided by the ISP server in the router is 192.168.1.2 through 192.168.1.254.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address.

Note: Ethernet and USB interfaces (and the wireless LAN interface on the CT-536+) share the same subnet since they are bridged within the router.

6. After entering your settings, select **Next** to display the following screen. The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

7. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.



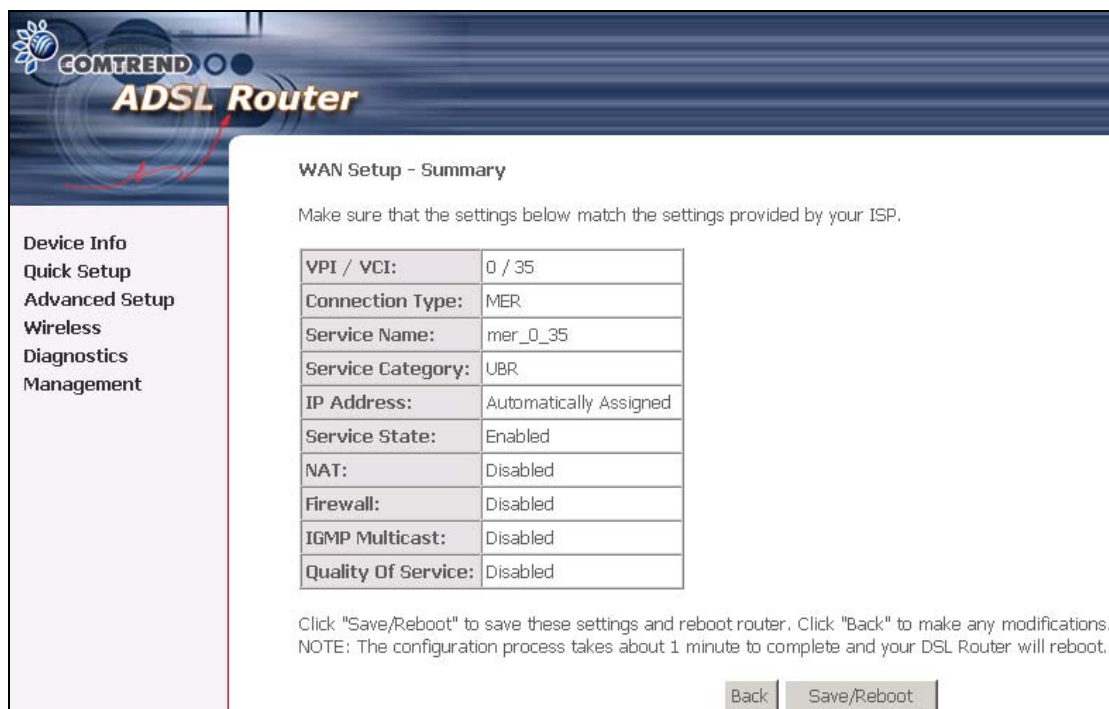
Wireless -- Setup

Enable Wireless ☒

Enter the wireless network name (also known as SSID).
 SSID:

[Back](#) [Next](#)

The following screen will be displayed.



COMTREND ADSL Router

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	0 / 35
Connection Type:	MER
Service Name:	mer_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
 NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-536+ is ready for operation and the LEDs display as described in the LED description tables.

5.2.3 IP Over ATM

To configure IP Over ATM,

1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type the VPI and VCI values provided by the ISP and click **Next**.
4. Select the IP over ATM (IPoA) radio button and click **Next**. The following screen appears.

The screenshot shows the 'WAN IP Settings' page of a COMTREND ADSL Router. The left sidebar contains a menu with 'Quick Setup' highlighted. The main content area has a title 'WAN IP Settings' and a subtitle 'Enter information provided to you by your ISP to configure the WAN IP settings.' Below this is a notice: 'Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.' The form includes fields for 'WAN IP Address' (123.124.125.126) and 'WAN Subnet Mask' (255.255.255.0). There are two main sections for optional settings: 'Use the following default gateway:' and 'Use the following DNS server addresses:'. The first section has checkboxes for 'Use IP Address' and 'Use WAN Interface' (selected), with a dropdown menu showing 'ipoa_0_35/ipa_0_35'. The second section has fields for 'Primary DNS server' and 'Secondary DNS server'. At the bottom right are 'Back' and 'Next' buttons.

Notice that DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup, and the DNS server addresses provided by the ISP.

5. Click **Next**. The following screen appears.

The screenshot shows the 'Network Address Translation Settings' page of a COMTREND ADSL Router. The left sidebar contains a menu with 'Quick Setup' highlighted. The main content area has a title 'Network Address Translation Settings' and a subtitle 'Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).' The form includes checkboxes for 'Enable NAT' and 'Enable Firewall'. Below these is a section 'Enable IGMP Multicast, and WAN Service' with checkboxes for 'Enable IGMP Multicast' and 'Enable WAN Service' (checked). There is a 'Service Name' field with the value 'ipoa_0_35'. At the bottom right are 'Back' and 'Next' buttons.

Enable NAT checkbox

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side (i.e the LAN side is using a public IP), this checkbox should be de-selected. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

Enable Firewall checkbox

If the firewall checkbox is selected, the Security submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main panel.

Enable Quality Of Service

Enabling IP QoS for a PVC improves performance for selected classes of applications. However, since IP QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

6. Click **Next** to display the following screen. The Device Setup page allows the user to configure the LAN interface IP address and DHCP server if the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the button Enable DHCP server on the LAN to enter the starting IP address and end IP address and DHCP lease time.

COMTREND
ADSL Router

Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

☐ Enable DHCP Server Relay

DHCP Server IP Address:

☐ Configure the second IP Address and Subnet Mask for LAN interface

The user must configure the IP Address and the Subnet Mask. To use the DHCP service on the LAN, select the **Enable DHCP server** checkbox, and enter the Start IP addresses, the End IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Note that the router's default IP address is 192.168.1.1 and the default private address range provided by ISP server in the router is 192.168.1.2 through 192.168.1.254.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address.

7. The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

8. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.

Wireless -- Setup

Enable Wireless ☒

Enter the wireless network name (also known as SSID).

SSID:

Back Next

The following screen will be displayed.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	0 / 35
Connection Type:	IPoA
Service Name:	ipoa_0_35
Service Category:	UBR
IP Address:	123.124.125.126
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

Back Save/Reboot

9. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-536+ is ready for operation and the LEDs display as described in the LED description tables.

5.2.4 Bridging

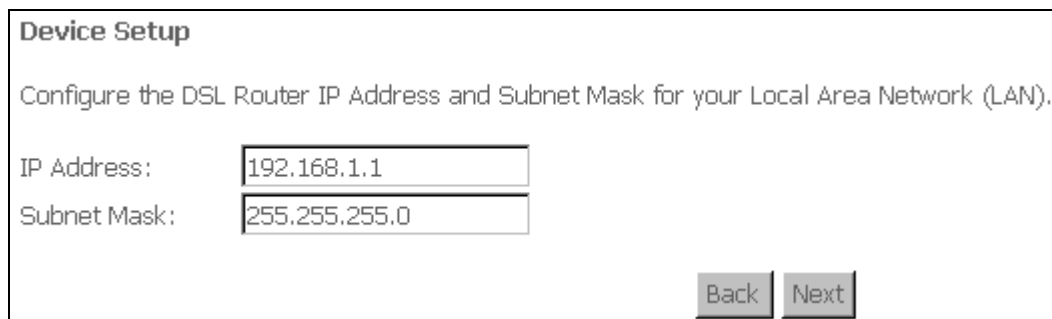
Select the bridging mode. To configure Bridging, do the following.

1. Select Quick Setup and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type in the VPI and VCI values provided by the ISP and click Next.
4. Select the Bridging radio button and click **Next**. The following screen appears.
To use the bridge service, tick the checkbox, Enable Bridge Service, and enter the service name.




The screenshot shows the COMTREND ADSL Router configuration interface. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main area has a header with the COMTREND logo and 'ADSL Router'. Below the header, it says 'Unselect the check box below to disable this WAN service'. There is a checkbox labeled 'Enable Bridge Service:' which is checked. Below it is a text field labeled 'Service Name:' containing the text 'br_0_35'. At the bottom right are 'Back' and 'Next' buttons.

5. Click the **Next** button to continue. Enter the IP address for the LAN interface. The default IP address is 192.168.1.1. The LAN IP interface in bridge operating mode is needed for local users to manage the ADSL router. Notice that there is no IP address for the WAN interface in bridge mode, and the remote technical support cannot access the ADSL router.



The screenshot shows the 'Device Setup' screen. It has a title 'Device Setup' and a subtitle 'Configure the DSL Router IP Address and Subnet Mask for your Local Area Network (LAN)'. There are two text input fields: 'IP Address:' with the value '192.168.1.1' and 'Subnet Mask:' with the value '255.255.255.0'. At the bottom right are 'Back' and 'Next' buttons.

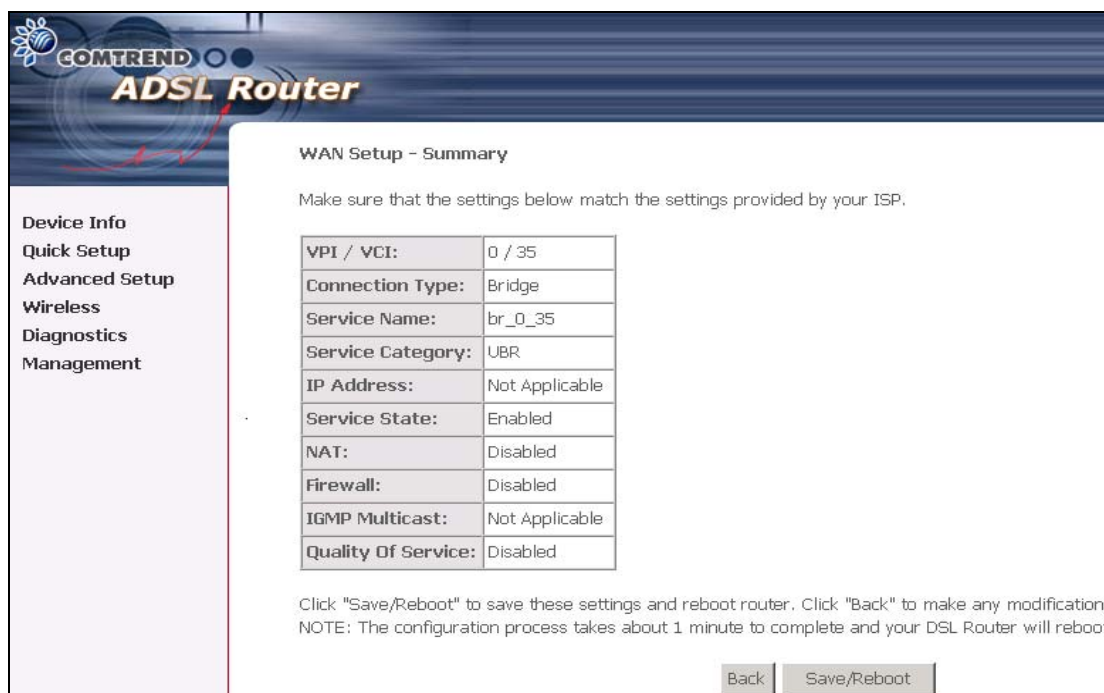
6. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.



The screenshot shows the 'Wireless -- Setup' configuration page of a COMTREND ADSL Router. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main area is titled 'Wireless -- Setup' and contains the following elements:

- 'Enable Wireless' with a checked checkbox.
- A text prompt: 'Enter the wireless network name (also known as SSID).' followed by an input field containing 'Comtrend'.
- 'Back' and 'Next' buttons at the bottom right.

The following screen will be displayed.



The screenshot shows the 'WAN Setup - Summary' configuration page of a COMTREND ADSL Router. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main area is titled 'WAN Setup - Summary' and contains the following elements:

- A note: 'Make sure that the settings below match the settings provided by your ISP.'
- A table summarizing the WAN configuration settings.
- A note at the bottom: 'Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications. NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.'
- 'Back' and 'Save/Reboot' buttons at the bottom right.

VPI / VCI:	0 / 35
Connection Type:	Bridge
Service Name:	br_0_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

Chapter 6 Advanced Setup

This chapter explains: WAN, LAN, Routing, DSL and Port Mapping.....

The screenshot shows the 'Wide Area Network (WAN) Setup' page of a COMTREND ADSL Router. On the left is a sidebar menu with options: Device Info, Quick Setup, Advanced Setup (highlighted), WAN, LAN, Routing, DSL, Port Mapping, Wireless, Diagnostics, and Management. The main content area has a title 'Wide Area Network (WAN) Setup' and instructions: 'Choose Add, Edit, or Remove to configure WAN interfaces. Choose Save/Reboot to apply the changes and reboot the system.' Below this is a table with columns: VPI/VCI, Con. ID, Category, Service, Interface, Protocol, Igmp, QoS, VlanId, State, Remove, and Edit. At the bottom of the table are three buttons: 'Add', 'Remove', and 'Save/Reboot'.

VPI/VCI	ATM VPI (0-255) / VCI (32-65535)
Con. ID	ID for WAN connection
Category	ATM service category, e.g. UBR, CBR...
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows bridge or router mode
IGMP	Shows enable or disable IGMP proxy
QoS	Shows enable or disable QoS
VlanID	<ul style="list-style-type: none"> This function means one can add an 802.1Q VLAN tag on PPPoE/MER or Bridge mode. <p>It means the packets are sent to WAN and a specific VlanID (802.1Q tag) will be added in the Ethernet header. The VlanID shows which 802.1Q tag will be added.</p>
State	Shows enable or disable WAN connection

6.1 WAN

COMTREND
ADSL Router

Device Info
Quick Setup
Advanced Setup
WAN
LAN
Routing

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	VlanId	State	Remove	Edit
---------	---------	----------	---------	-----------	----------	------	-----	--------	-------	--------	------

For further information on WAN please reference section: 4.1, Page 18.

6.2 LAN

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address: Enter the IP address for the LAN port.

Subnet Mask: Enter the subnet mask for the LAN port.

Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address:

Subnet Mask:

☒ Enable IGMP Snooping

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

☐ Enable DHCP Server Relay

DHCP Server IP Address:

☐ Configure the second IP Address and Subnet Mask for LAN interface

Ethernet Media Type

Port 1:

Port 2:

Port 3:

Port 4:

IGMP Snooping: Tick the box if required.

To configure a secondary IP address for the LAN port, click the box as shown below.

☒ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

Ethernet Media Type

Port 1:

Port 2:

Port 3:

Port 4:

IP Address: Enter the secondary IP address for the LAN port.

Subnet Mask: Enter the secondary subnet mask for the LAN port.

6.3 NAT

To display the NAT function, you need to enable the NAT feature in the WAN Setup.

6.3.1 Virtual Servers

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.



The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with categories: Device Info, Advanced Setup, and Management. Under Advanced Setup, 'Virtual Servers' is highlighted in red. The main content area is titled 'NAT -- Virtual Servers Setup'. It contains a descriptive paragraph about Virtual Servers and two buttons, 'Add' and 'Remove'. Below these is a table with 8 columns: Server Name, External Port Start, External Port End, Protocol, Internal Port Start, Internal Port End, Server IP Address, and Remove. The table is currently empty.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	--------

To add a Virtual Server, simply click the **Add** button. The following will be displayed.

COMTREND ADSL Router

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified. Remaining number of entries that can be configured:32

Server Name:
☒ Select a Service: Select One
☐ Custom Server:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>

Select a Service Or Custom Server	User should select the service from the list. Or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

6.3.2 Port Triggering

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

COMTREND ADSL Router

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Add Remove

Application	Trigger	Open	Remove			
Name	Protocol	Port Range	Protocol	Port Range		
		Start	End	Start	End	

To add a Trigger Port, simply click the Add button. The following will be displayed.

COMTREND ADSL Router

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

Remaining number of entries that can be configured:32

Application Name:

☒ Select an application: Select One

☐ Custom application:

Save/Apply

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Save/Apply

Select an Application Or Custom Application	User should select the application from the list. Or User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Protocol	User can select from: TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Protocol	User can select from: TCP, TCP/UDP or UDP.

6.3.3 DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.



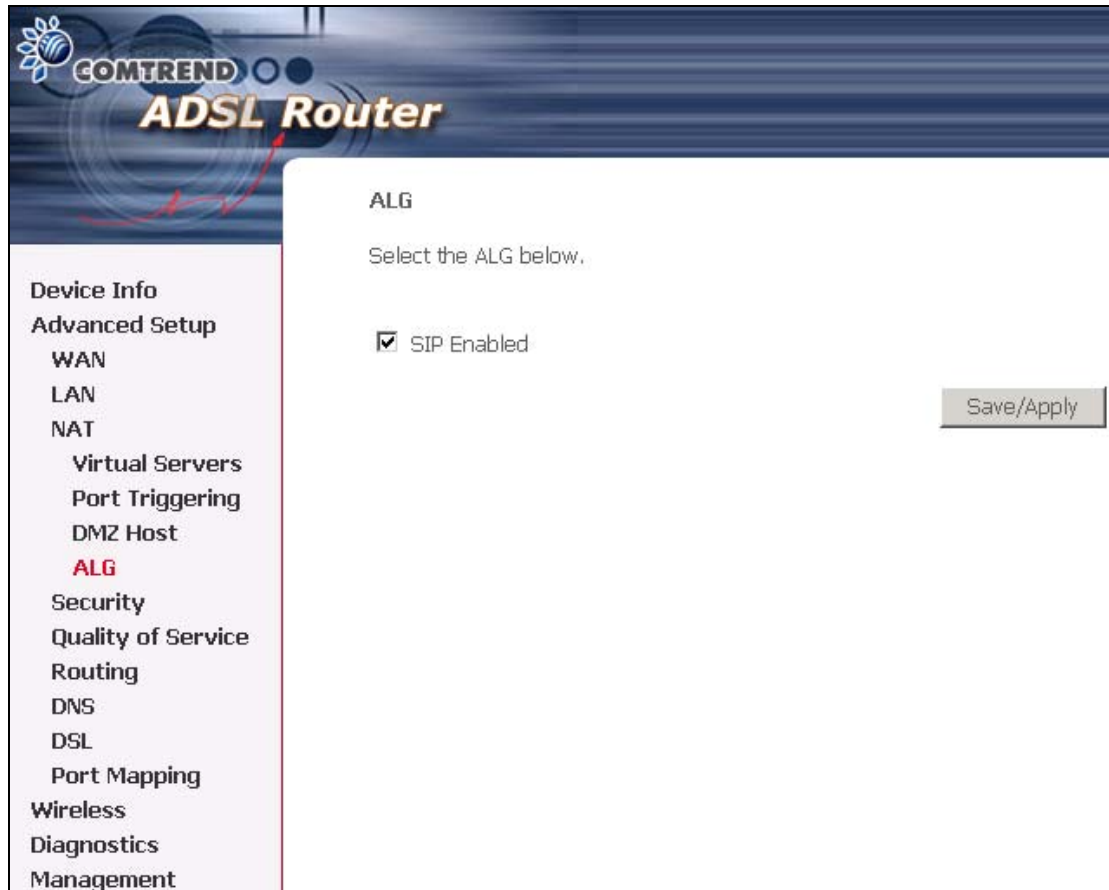
The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with options: Device Info, Advanced Setup, WAN, LAN, NAT, Virtual Servers, Port Triggering, **DMZ Host** (highlighted in red), ALG, Security, Quality of Service, Routing, DNS, DSL, Port Mapping, Wireless, Diagnostics, and Management. The main content area is titled "NAT -- DMZ Host". It contains the following text: "The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.", "Enter the computer's IP address and click 'Apply' to activate the DMZ host.", and "Clear the IP address field and click 'Apply' to deactivate the DMZ host." Below this text is a label "DMZ Host IP Address:" followed by an empty text input field. To the right of the input field is a "Save/Apply" button.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

6.3.4 ALG

SIP ALG is Application layer gateway. If the user has an IP phone(SIP) or VoIP gateway(SIP) behind the ADSL router, the SIP ALG can help VoIP packet passthrough the router (NAT enabled).



Note: SIP (Session Initiation Protocol, RFC3261) is the protocol of choice for most VoIP (Voice over IP) phones to initiate communication. This ALG is only valid for SIP protocol running on UDP port 5060.

6.4 Security

To display the Security function, you need to enable the firewall feature in the WAN Setup.

6.4.1 IP Filtering

IP filtering allows you to create a filter rule to identify outgoing/incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Outgoing

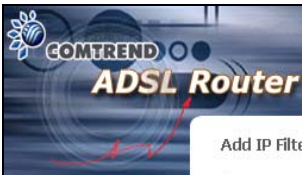
Note: The default setting for Outgoing is Blocked.



The screenshot shows the Comtrend ADSL Router web interface. On the left is a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Security, IP Filtering (highlighted), Outgoing (highlighted in red), Incoming, Parental Control, Quality of Service, Routing, DNS, DSL, Port Mapping, Wireless, Diagnostics, and Management. The main content area is titled 'Outgoing IP Filtering Setup'. It contains the text: 'By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters. Choose Add or Remove to configure outgoing IP filters.' Below this text is a table with the following headers: Filter Name, Protocol, Source Address / Mask, Source Port, Dest. Address / Mask, Dest. Port, and Remove. The table is currently empty. Below the table are two buttons: 'Add' and 'Remove'.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
-------------	----------	-----------------------	-------------	----------------------	------------	--------

To add a filtering rule, simply click the Add button. The following screen will be displayed.



Device Info
Advanced Setup
WAN
LAN
NAT
Security
 IP Filtering
 Outgoing
 Incoming
 Parental Control
 Quality of Service
Routing
DNS
DSL
Port Mapping
Wireless
Diagnostics
Management

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Filter Name	Type a name for the filter rule.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.

Incoming

Note: The default setting for Incoming is Accepted.

The screenshot shows the 'Incoming IP Filtering Setup' page. On the left is a navigation menu with categories: Device Info, Advanced Setup (WAN, LAN, NAT), Security (IP Filtering, Outgoing, Incoming, Parental Control), Quality of Service, Routing, DNS, DSL, Port Mapping, Wireless, Diagnostics, and Management. The 'Incoming' option under Security is highlighted. The main content area is titled 'Incoming IP Filtering Setup' and contains the following text: 'By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.' Below this is the instruction 'Choose Add or Remove to configure incoming IP filters.' and a table with the following headers: Filter Name, VPI/VCI, Protocol, Source Address / Mask, Source Port, Dest. Address / Mask, Dest. Port, and Remove. Below the table are 'Add' and 'Remove' buttons.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
-------------	---------	----------	-----------------------	-------------	----------------------	------------	--------

To add a filtering rule, simply click the Add button. The following screen will be displayed.

The screenshot shows the 'Add IP Filter -- Incoming' page. The left navigation menu is the same as the previous screenshot, with 'Incoming' highlighted. The main content area is titled 'Add IP Filter -- Incoming' and contains the following text: 'The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.' Below this are input fields for: Filter Name, Protocol (a dropdown menu), Source IP address, Source Subnet Mask, Source Port (port or port:port), Destination IP address, Destination Subnet Mask, and Destination Port (port or port:port). Below these fields is a section titled 'WAN Interfaces (Configured in Routing mode and with firewall enabled only)' with the instruction 'Select at least one or multiple WAN interfaces displayed below to apply this rule.' There are two checkboxes: 'Select All' (checked) and 'mer_0_35/has_0_35' (checked). At the bottom right is a 'Save/Apply' button.

To configure the parameters, please reference **Outgoing** table above.

6.4.2 Parental Control

Parental control: allows parents, schools, and libraries to set access times for Internet use.

COMTREND ADSL Router

Time of Day Restrictions -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>											

To add a parental control, simply click the Add button. The following screen will be displayed.

COMTREND ADSL Router

Time of Day Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name:

☒ Browser's MAC Address:

☐ Other MAC Address:

Days of the week: ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Click to select: ☐ ☐ ☐ ☐ ☐ ☐ ☐

Start Blocking Time (hh:mm):

End Blocking Time (hh:mm):

Username:	Name of the Filter.
MAC:	Set the MAC address to access the Internet.
Mon, Tue, Wed, Thu, Fri, Sat, Sun:	Set which days that will have block restrictions to Internet access.
Start, Stop:	The time when restrictions start and stop.

6.5 Quality of Service

To display the QoS function, you need to enable the QoS feature in the WAN Setup.

The screenshot shows the 'Quality of Service Setup' page of a COMTREND ADSL Router. The left sidebar contains a menu with options: Device Info, Advanced Setup (WAN, LAN, NAT, Security, Quality of Service, Routing, DNS, DSL, Port Mapping), Wireless, Diagnostics, and Management. The 'Quality of Service' option is highlighted. The main content area is titled 'Quality of Service Setup' and includes the instruction: 'Choose Add or Remove to configure network traffic classes.' Below this is a table with columns for MARK and TRAFFIC CLASSIFICATION RULES. The MARK columns are Class Name, Priority, IP Precedence, IP Type of Service, and WAN 802.1p. The TRAFFIC CLASSIFICATION RULES columns are divided into SET-1 (Lan Port, Protocol, Source Addr./Mask, Source Port, Dest. Addr./Mask, Dest. Port) and SET-2 (802.1p). A 'Remove' column is also present. Below the table are 'Add' and 'Remove' buttons.

MARK					TRAFFIC CLASSIFICATION RULES								
					SET-1						SET-2		
Class Name	Priority	IP Precedence	IP Type of Service	WAN 802.1p	Lan Port	Protocol	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	802.1p	Remove	

Choose **Add** to configure network traffic classes. The following screen will be displayed:

The screenshot shows the 'Add Network Traffic Class Rule' page of a COMTREND ADSL Router. The left sidebar is the same as the previous screenshot, with 'Quality of Service' highlighted. The main content area is titled 'Add Network Traffic Class Rule' and includes the instruction: 'The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.' Below this is a 'Traffic Class Name:' field. The next section is 'Assign Priority and/or IP Precedence and/or Type Of Service for the class', with the instruction: 'If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet will be overwritten by the selected value.' This section contains four dropdown menus: 'Assign ATM Transmit Priority:', 'Mark IP Precedence:', 'Mark IP Type Of Service:', and 'Mark 802.1p if 802.1q is enabled on WAN:'. The next section is 'Specify Traffic Classification Rules', with the instruction: 'Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.' This section contains two sets of conditions. SET-1 conditions include: 'Physical LAN Port:', 'Protocol:', 'Source IP Address:', 'Source Subnet Mask:', 'UDP/TCP Source Port (port or port:port):', 'Destination IP Address:', 'Destination Subnet Mask:', and 'UDP/TCP Destination Port (port or port:port):'. SET-2 conditions include: '802.1p Priority:'. A 'Save/Apply' button is at the bottom right.

The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name	Enter name for traffic class.
Assign ATM Transmit Priority	Select Low, Medium or High.
Mark IP Precedence	<p>Select between 0-7. The lower the digit shows the higher the priority</p> <p>If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.</p> <p>Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.</p>
Mark IP Type Of Service	<p>Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay</p> <p>If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.</p> <p>Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.</p>
Mark 802.1p if 802.1q is enabled on WAN	Select between 0-7.

Specify Traffic Classification Rules

Enter the following conditions either for physical LAN/Wireless port or for IP level, SET-1, or for IEEE 802.1p, SET-2

SET-1	
Physical LAN Port	User can select from: ENET, ENET(1-4), USB or Wireless.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.
SET-2	
802.1p Priority	Select between 0-7.
Traffic Class Name	Enter name for traffic class
Priority	Select Low, Medium or High.
IP Precedence	Select between 0-7. The lower the digit shows the higher the priority
Mark IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay
Physical LAN Port	User can select from: ENET, ENET(1-4), USB, or Wireless.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

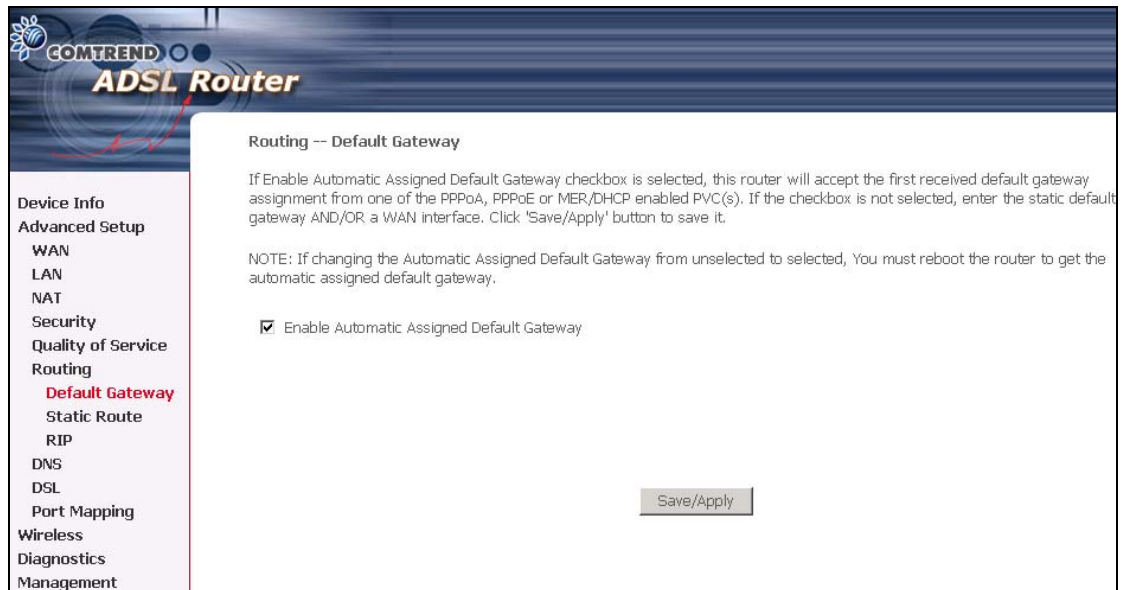
6.6 Routing

The Routing dialog box allows you to configure Default gateway, Static Route and RIP.

6.6.1 Default Gateway

If '**Enable Automatic Assigned Default Gateway**' checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.



The screenshot displays the Comtrend ADSL Router web interface. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service, Routing, Default Gateway (highlighted in red), Static Route, RIP, DNS, DSL, Port Mapping, Wireless, Diagnostics, and Management. The main content area is titled 'Routing -- Default Gateway'. It contains a paragraph explaining the 'Enable Automatic Assigned Default Gateway' checkbox. Below this, the checkbox is checked. A 'Save/Apply' button is located at the bottom right of the main content area.

COMTREND
ADSL Router

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
Default Gateway
Static Route
RIP
DNS
DSL
Port Mapping
Wireless
Diagnostics
Management

Routing -- Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

☒ Enable Automatic Assigned Default Gateway

Save/Apply

6.6.2 Static Route

Choose **Static Route** to display the Static Route screen. The Static Route screen lists the configured static routes, and allows configuring static routes. Choose **Add** or **Remove** to configure the static routes.

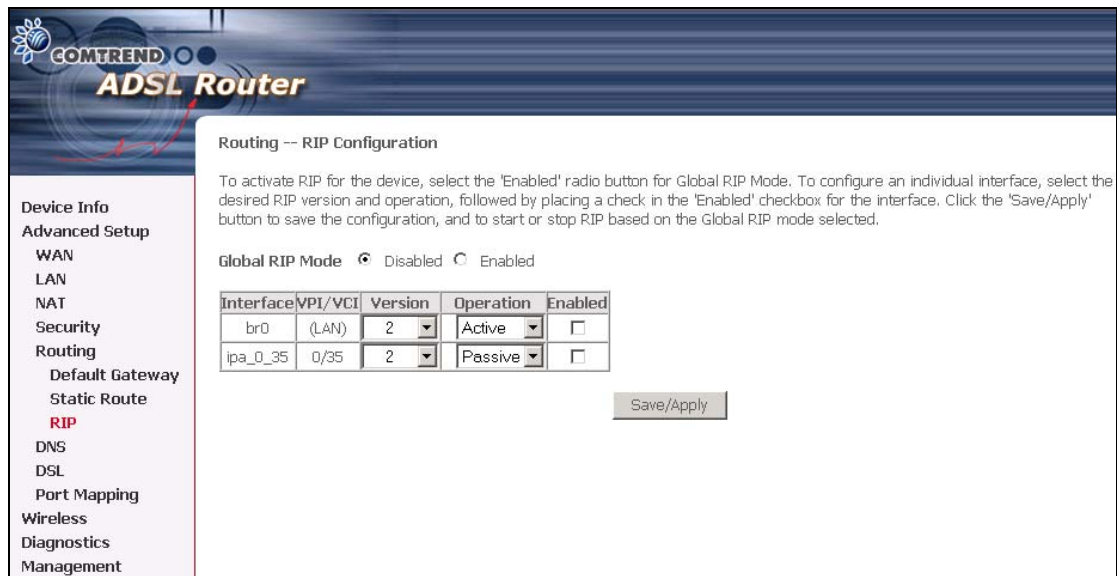
The screenshot shows the Comtrend ADSL Router web interface. On the left is a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service, Routing (highlighted), Default Gateway, Static Route (highlighted in red), RIP, DNS, DSL, Port Mapping, Wireless, Diagnostics, and Management. The main content area is titled "Routing -- Static Route (A maximum 32 entries can be configured)". It contains a table with headers: Destination, Subnet Mask, Gateway, Interface, and Remove. Below the table are two buttons: "Add" and "Remove".

To add static route, click the **Add** button to display the following screen. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **Save/Apply** to add the entry to the routing table.

The screenshot shows the "Routing -- Static Route Add" screen. It includes the same navigation menu as the previous screen. The main content area has a title "Routing -- Static Route Add" and a instruction: "Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click 'Save/Apply' to add the entry to the routing table." Below this are input fields for "Destination Network Address:" and "Subnet Mask:". There are two checkboxes: "Use Gateway IP Address" (unchecked) and "Use Interface" (checked). The "Use Interface" checkbox is followed by a dropdown menu showing "mer_0_35/nas_0_35". At the bottom right is a "Save/Apply" button.

6.6.3 RIP

To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.



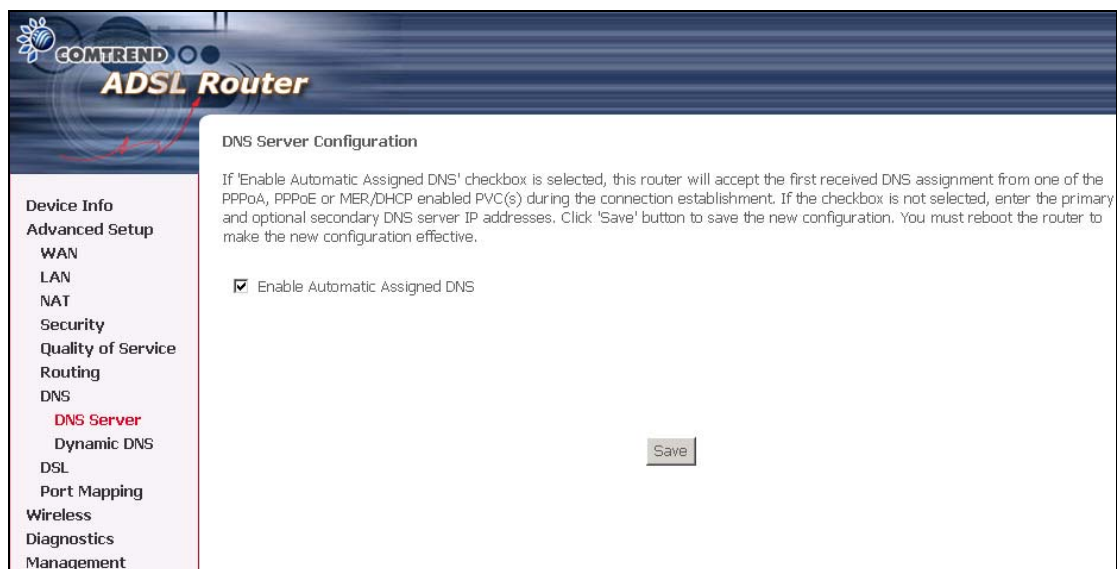
The screenshot shows the 'Routing -- RIP Configuration' page of a COMTREND ADSL Router. The left sidebar contains a menu with options: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Routing (selected), Default Gateway, Static Route, RIP (highlighted in red), DNS, DSL, Port Mapping, Wireless, Diagnostics, and Management. The main content area has a title 'Routing -- RIP Configuration' and a descriptive text: 'To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.' Below this text, the 'Global RIP Mode' is set to 'Disabled' (radio button). A table lists two interfaces: 'br0' (LAN) and 'ipa_0_35' (0/35). Both are configured with 'Version' 2. 'br0' has 'Operation' set to 'Active' and 'Enabled' checkbox unchecked. 'ipa_0_35' has 'Operation' set to 'Passive' and 'Enabled' checkbox unchecked. A 'Save/Apply' button is located at the bottom right of the configuration area.

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	<input type="checkbox"/>
ipa_0_35	0/35	2	Passive	<input type="checkbox"/>

6.7 DNS

6.7.1 DNS Server

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.



The screenshot shows the web interface of a COMTREND ADSL Router. The top header features the COMTREND logo and the text 'ADSL Router'. On the left is a vertical navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service, Routing, DNS, **DNS Server** (highlighted in red), Dynamic DNS, DSL, Port Mapping, Wireless, Diagnostics, and Management. The main content area is titled 'DNS Server Configuration'. It contains a paragraph explaining the 'Enable Automatic Assigned DNS' checkbox. Below this text is a checkbox labeled 'Enable Automatic Assigned DNS' which is checked. At the bottom right of the main content area is a 'Save' button.

COMTREND
ADSL Router

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DSL
Port Mapping
Wireless
Diagnostics
Management

DNS Server Configuration

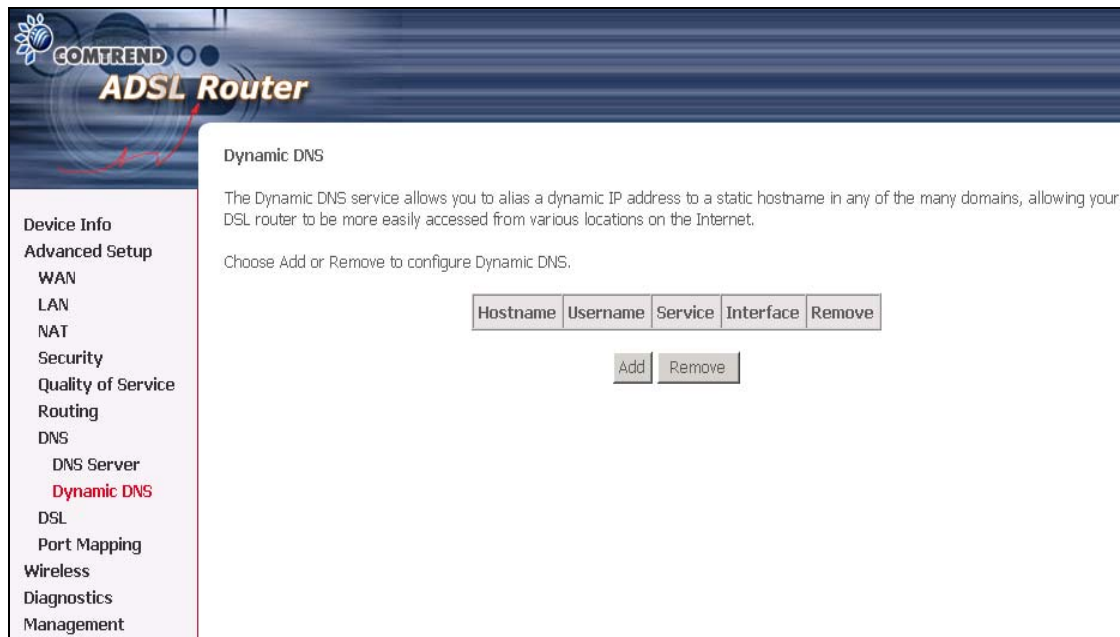
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.

☒ Enable Automatic Assigned DNS


Save

6.7.2 Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.



To add a dynamic DNS service, simply click the Add button. The following screen will be displayed:



Device Info
Advanced Setup
WAN
LAN
NAT
Parental Control
Quality of Service
Routing
DNS
 DNS Server
 Dynamic DNS
DSL
Port Mapping
Wireless
Diagnostics
Management

Add dynamic DDNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider

Hostname

Interface

DynDNS Settings

Username

Password

D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name for the dynamic DNS server.
Interface	Select the interface from the list
Username	Enter the username for the dynamic DNS server.
Password	Enter the password for the dynamic DNS server.

6.8 DSL

To access the DSL settings, First click On **Advanced Setup** and then click on **DSL**. The DSL Settings dialog box allows you to select an appropriate modulation mode.

COMTREND ADSL Router

DSL Settings

Select the modulation below.

- ☒ G.Dmt Enabled
- ☒ G.lite Enabled
- ☒ T1.413 Enabled
- ☒ ADSL2 Enabled
- ☒ AnnexL Enabled
- ☒ ADSL2+ Enabled
- ☒ AnnexM DISABLED

Select the phone line pair below.

- ☒ Inner pair
- ☐ Outer pair

Capability

- ☒ Bitswap Enable
- ☐ SRA Enable

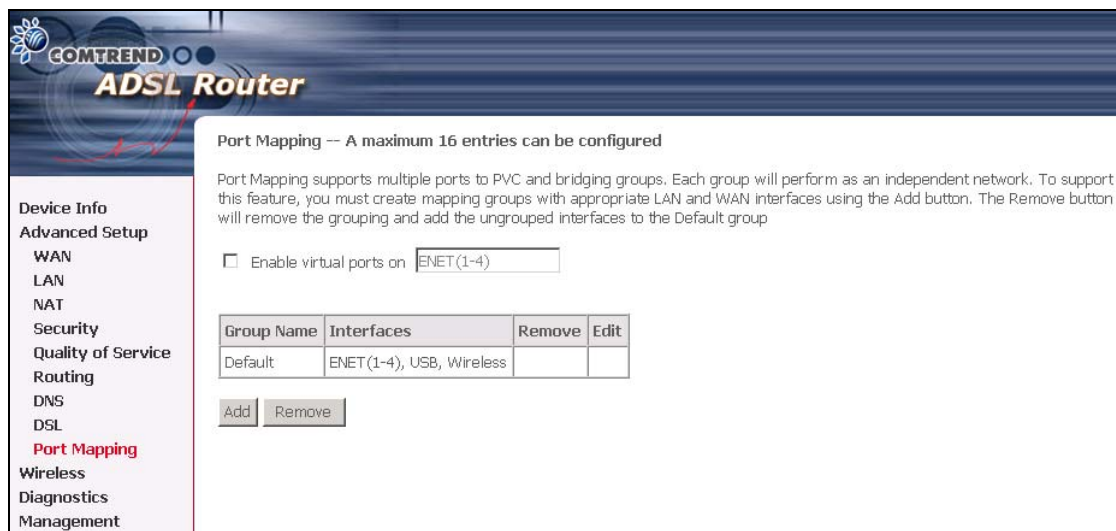
Save/Apply

Option	Description
G.dmt Enabled	Sets G.Dmt if you want the system to use G.Dmt mode.
G.Lite Enabled	Sets G.Lite if you want the system to use G.Lite mode.
T1.413 Enabled	Sets the T1.413 if you want the system to use only T1.413 mode.
ADSL2 Enabled	The device can support the functions of the ADSL2.
AnnexL Enabled	The device can support/enhance the long loop test.
ADSL2+ Enabled	The device can support the functions of the ADSL2+.
AnnexM DISABLED	Covers a higher "upstream" data rate version, by making use of some of the downstream channels.
Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswaping function
SRA Enable	Allows seamless rate adaptation

6.9 Port Mapping

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group.

As shown below, when you tick the Enable virtual ports on, all of the LAN interfaces will be grouped together as a default.



COMTREND ADSL Router

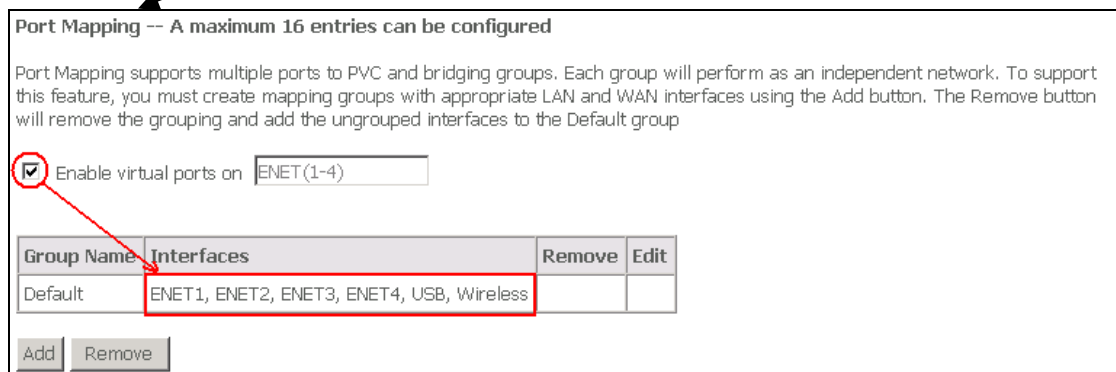
Port Mapping -- A maximum 16 entries can be configured

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group

☐ Enable virtual ports on ENET(1-4)

Group Name	Interfaces	Remove	Edit
Default	ENET(1-4), USB, Wireless		

Add Remove



Port Mapping -- A maximum 16 entries can be configured


Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group

☒ Enable virtual ports on ENET(1-4)

Group Name	Interfaces	Remove	Edit
Default	ENET1, ENET2, ENET3, ENET4, USB, Wireless		

Add Remove

To add a Port Mapping group, simply click the Add button.



Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Port Mapping
Wireless
Diagnostics
Management

Port Mapping Configuration

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. Click Save/Apply button to make the changes effective immediately

Note that the selected interfaces will be removed from their existing groups and added to the new group.

Group Name:

Grouped Interfaces		Available Interfaces
<div></div>	<div>-></div> <div><-</div>	<div>ENET1 ENET2 ENET3 ENET4 USB Wireless</div>

Save/Apply

To create a group from the list, first enter the group name and then select from the available interfaces on the list.

Chapter 7 Wireless

The Wireless dialog box allows you to enable the wireless capability, hide the access point, set the wireless network name and restrict the channel set.

The screenshot shows the 'Wireless -- Basic' configuration page of a Comtrend ADSL Router. The left sidebar contains a menu with 'Device Info', 'Advanced Setup', 'Wireless', 'Basic', 'Security', 'MAC Filter', 'Wireless Bridge', 'Advanced', 'Station Info', 'Diagnostics', and 'Management'. The 'Wireless' and 'Basic' items are highlighted with a red box. The main content area is titled 'Wireless -- Basic' and contains the following text: 'This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply" to configure the basic wireless options.'

Below the text are the following configuration options:

- ☒ Enable Wireless
- ☐ Hide Access Point
- SSID:
- BSSID:
- Country:

A 'Save/Apply' button is located at the bottom right of the configuration area.

7.1 Wireless Basic Screen

The Basic option allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

Click **Apply** to configure the basic wireless options.

This screenshot is identical to the one above, showing the 'Wireless -- Basic' configuration page of a Comtrend ADSL Router. The left sidebar menu is the same, with 'Wireless' and 'Basic' highlighted. The main content area contains the same text and configuration options: 'Enable Wireless' (checked), 'Hide Access Point' (unchecked), SSID: 'Comtrend', BSSID: '00:03:C9:43:0A:51', and Country: 'ALL'. A 'Save/Apply' button is at the bottom right.

Option	Description
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wireless.
Hide Access Point	<p>Select Hide Access Point to protect ADSL router access point from detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be de-selected.</p> <p>The station will not discover this access point. To connect a station to the available access points, the station must manually add this access point name in its wireless configuration.</p> <p>In Windows XP, go to the Network>Programs function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.</p>
SSID	<p>Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.</p> <p>The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.</p>
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	<p>A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range:</p> <ul style="list-style-type: none"> ● US= worldwide ● Japan=1-14 ● Jordan= 10-13 ● Israel= 1-13

7.1.1 Security

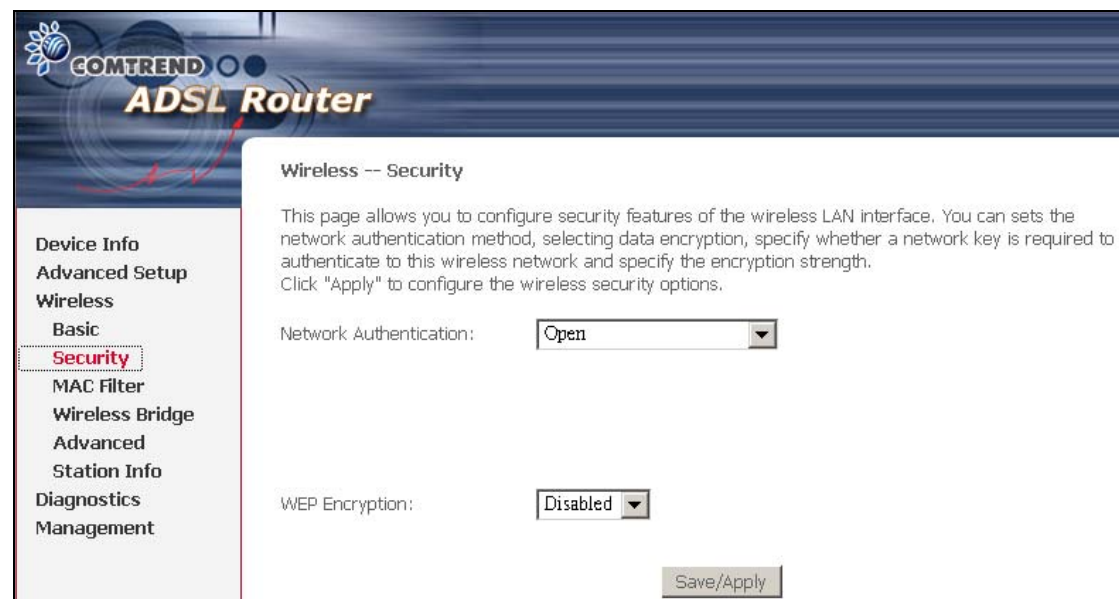
Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The system that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then sends back a frame that indicates whether it recognizes the identity of the sending station.

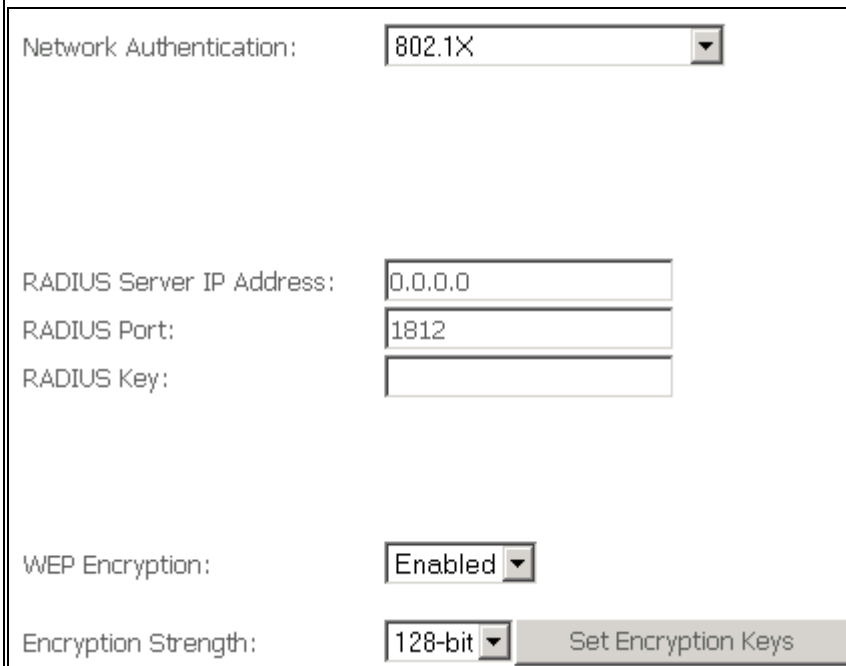
Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from 802.11 wireless network communications channel.

The following screen appears when Security is selected. The Security page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Click **Apply** to configure the wireless security options.



The screenshot shows the 'Wireless -- Security' configuration page of a COMTREND ADSL Router. The page has a dark blue header with the router's logo and name. On the left, a sidebar lists navigation options: Device Info, Advanced Setup, Wireless, Basic, Security (highlighted with a red border), MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, and Management. The main content area is titled 'Wireless -- Security' and contains a descriptive paragraph: 'This page allows you to configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply" to configure the wireless security options.' Below this text are two configuration fields: 'Network Authentication:' with a dropdown menu set to 'Open', and 'WEP Encryption:' with a dropdown menu set to 'Disabled'. At the bottom right, there is a 'Save/Apply' button.

Option	Description
Network Authentication	<p>It specifies the network authentication. When this checkbox is selected, it specifies that a network key be used for authentication to the wireless network. If the Network Authentication (Shared mode) checkbox is not shared (that is, if open system authentication is used), no authentication is provided. Open system authentication only performs identity verifications.</p> <p>Different authentication type pops up different settings requests.</p> <p>Choosing 802.1X, enter RADIUS Server IP address, RADIUS Port, and RADIUS key.</p> <p>Also, enable WEP Encryption and the Encryption Strength.</p> <div data-bbox="437 909 1286 1572">  <p>Network Authentication: 802.1X</p> <p>RADIUS Server IP Address: 0.0.0.0</p> <p>RADIUS Port: 1812</p> <p>RADIUS Key:</p> <p>WEP Encryption: Enabled</p> <p>Encryption Strength: 128-bit Set Encryption Keys</p> </div> <p>Choosing WPA, you must enter WPA Group Rekey Interval.</p>

	<div data-bbox="491 203 1396 660"> <p>Network Authentication: WPA</p> <p>WPA Group Rekey Interval: 0</p> <p>RADIUS Server IP Address: 0.0.0.0</p> <p>RADIUS Port: 1812</p> <p>RADIUS Key: </p> <p>WPA Encryption: TKIP</p> <p>WEP Encryption: Disabled</p> </div> <p>Choosing WPA-PSK, you must enter WPA Pre-Shared Key and Group Rekey Interval.</p> <div data-bbox="443 770 1396 1146"> <p>Network Authentication: WPA-PSK</p> <p>WPA Pre-Shared Key: Click here to display</p> <p>WPA Group Rekey Interval: 0</p> <p>WPA Encryption: TKIP</p> <p>WEP Encryption: Disabled</p> </div>
WEPEncryption	It specifies that a network key is used to encrypt the data is sent over the network. When this checkbox is selected, it enables data encryption and prompts the Encryption Strength drop-down menu. Data Encryption (WEP Enabled) and Network Authentication use the same key.
Encryption strength	<p>A session's key strength is proportional to the number of binary bits comprising the session key file. This means that session keys with a greater number of bits have a greater degree of security, and are considerably more difficult to forcibly decode. This drop-down menu sets either a 64 8-bit (5-ASCII characters or 10-hexadecimal characters) or 128 8-bit (13-ASCII characters or 26-hexadecimal characters) key.</p> <p>If you set a minimum 128-bit key strength, users attempting to establish a secure communications channel with your server must use a browser capable of communicating with a 128-bit session key.</p> <p>The Encryption Strength settings do not display unless the network Authentication (shared Mode) check box is selected.</p>

7.1.2 MAC Filter

This MAC Filter page allows access to be restricted/allowed based on a MAC address. All NICs have a unique 48-bit MAC address burned into the ROM chip on the card. When MAC address filtering is enabled, you are restricting the NICs that are allowed to connect to your access point. Therefore, an access point will grant access to any computer that is using a NIC whose MAC address is on its “allows” list.

Wi-Fi routers and access points that support MAC filtering let you specify a list of MAC addresses that may connect to the access point, and thus dictate what devices are authorized to access the wireless network. When a device is using MAC filtering, any address not explicitly defined will be denied access.

MAC Restrict mode: **Off**- disables MAC filtering; **Allow** – permits **access** for the specified MAC address; **deny**; reject access of the specified MAC address, then click the **SET** button.

To delete an entry, select the entry at the bottom of the screen and then click the **Remove** button, located on the right hand side of the screen.

To add a MAC entry, click **Add** and enter MAC address



After choosing the Add button, the following screen appears. Enter the MAC address and click **Apply** to add the MAC address to the wireless MAC address filters.

COMTREND ADSL Router

Wireless -- MAC Filter

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

MAC Address:

Save/Apply

Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management

COMTREND ADSL Router

Wireless -- MAC Filter

MAC Restrict Mode: ☒ Disabled ☐ Allow ☐ Deny

MAC Address	Remove
AB:0A:00:12:12:AB	<input type="checkbox"/>

Add Remove

Device Info
Quick Setup
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info

Option	Description
MAC Restrict Mode	Radio buttons that allow settings of; Off: MAC filtering function is disabled. Allow: Permits PCs with listed MAC addresses to connect to the access point. Deny: Prevents PCs with listed MAC from connecting to the access point.
MAC Address	Lists the MAC addresses subject to the Off, Allow, or Deny instruction. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. The maximum number of MAC addresses that can be added is 60.

7.1.3 Wireless Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict, which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

COMTREND ADSL Router

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Save/Apply" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Option	Description
AP Mode	Access Point Wireless Bridge
Bridge Restrict	Enabled Enabled (Scan) Disabled

7.1.4 Advanced

The Advanced page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click **Apply** to configure the advanced wireless options.

The screenshot shows the 'Wireless -- Advanced' configuration page of a COMTREND ADSL Router. The page has a left sidebar with navigation links: Device Info, Advanced Setup, Wireless, Basic, Security, MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, and Management. The main content area is titled 'Wireless -- Advanced' and contains a descriptive paragraph: 'This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply" to configure the advanced wireless options.' Below this text are various configuration fields: AP Isolation (Off), Band (2.4GHz - 802.11g), Channel (11), Rate (Auto), Multicast Rate (Auto), Basic Rate (Default), Fragmentation Threshold (2346), RTS Threshold (2347), DTIM Interval (1), Beacon Interval (100), XPress™ Technology (Disabled), 54g™ Mode (54g Auto), 54g Protection (Auto), and WMM(Wi-Fi Multimedia) (Disabled). A 'Save/Apply' button is located at the bottom right of the configuration area.

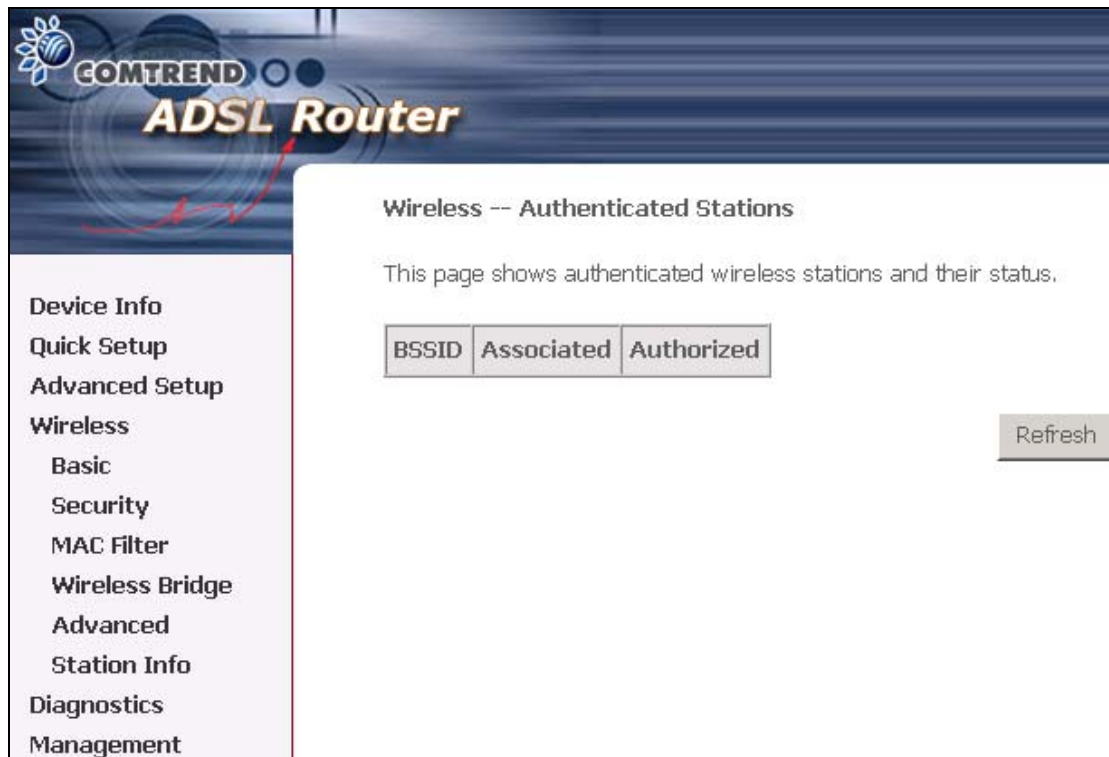
Option	Description
AP Isolation	Select On or Off. By enabling this feature, wireless clients associated with the Access Point will be able to connect to each other.
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)

Channel	Drop-down menu that allows selection of specific channel.
Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting multicast packet transmit rate.
Basic Rate	Setting basic transmit rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Beacon Interval	The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)
Xpress TM Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
Wireless Media Extension	Provides an interim QoS solution for 802.11 networks until the release of 802.11e. WRAP (Wireless Robust Authenticated Protocol) An encryption protocol in the 802.11i standard. WRAP is based upon the Offset Codebook (OCB) mode of AES. WRAP is being replaced with CCMP.
54g TM Mode	Select the mode to 54g Auto for the widest compatibility. Select the mode to 54g Performance for the fastest performance among 54g certified equipment. Set the mode to 54g LRS if you are experiencing difficulty with legacy 802.11b equipment.
54g Protection	In Auto mode the router will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
WMM (Wi-Fi Multimedia)	This is a standard that is meant to improve audio, video and voice applications transmitted over a wireless network.

7.1.5 Station Info

This page shows authenticated wireless stations and their status.

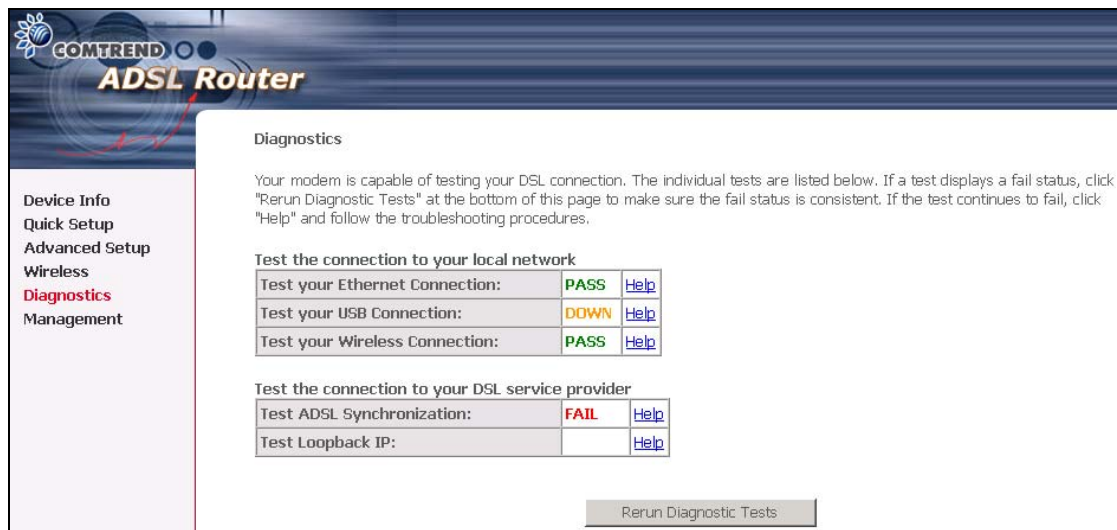


BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.

Chapter 8 Diagnostics

The Diagnostics menu provides feedback on the connection status of the CT-536+ and the ADSL link. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.

This is the default screen for the device.



Test	Description
Ethernet Connection	Pass: indicates that the Ethernet interface from your computer is connected to the LAN port of your DSL Router. A flashing or solid green LAN LED on the router also signifies that an Ethernet connection is present and that this test is successful. Fail: Indicates that the DSL Router does not detect the Ethernet interface on your computer.
USB connection	Pass: Indicates that the USB interface from your computer is connected to the LAN port of your DSL router. Down: Indicates that the DSL Router does not detect the USB interface on your computer.
Wireless connection	Pass: Indicates that the Wireless interface from your computer is connected to the wireless network.

	Down: Indicates that the DSL Router does not detect the wireless network.
ADSL Synchronization	<p>Pass: Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid WAN LED on the router also indicates the detection of a DSL signal from the telephone company.</p> <p>Fail: indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The WAN LED will stop blinking (i.e. training) and the LED will stop illuminating (i.e. go blank).</p>
ISP Connection	<p>Pass: Indicates we can access the WAN service like the Gateway and DNS.</p> <p>Fail: Indicates we cannot access the WAN side.</p>

If router mode is PPPoE the following screen will be displayed (for your reference).

The screenshot shows the 'pppoe_0_35_1 Diagnostics' page on a COMTREND ADSL Router. The page has a left sidebar with navigation links: Device Info, Advanced Setup, Wireless, **Diagnostics**, and Management. The main content area displays test results for three categories: local network, DSL service provider, and Internet service provider. Each category has a table of tests with their status (PASS, DOWN, FAIL) and a 'Help' link. At the bottom, there are 'Test' and 'Test With OAM F4' buttons.

COMTREND ADSL Router

pppoe_0_35_1 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your Ethernet Connection:	PASS	Help
Test your USB Connection:	DOWN	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	FAIL	Help
Test ATM OAM F5 end-to-end ping:	FAIL	Help

Test the connection to your Internet service provider

Test PPP server connection:	FAIL	Help
Test authentication with ISP:	PASS	Help
Test the assigned IP address:	FAIL	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	PASS	Help
Test Loopback IP:		Help

Test Test With OAM F4

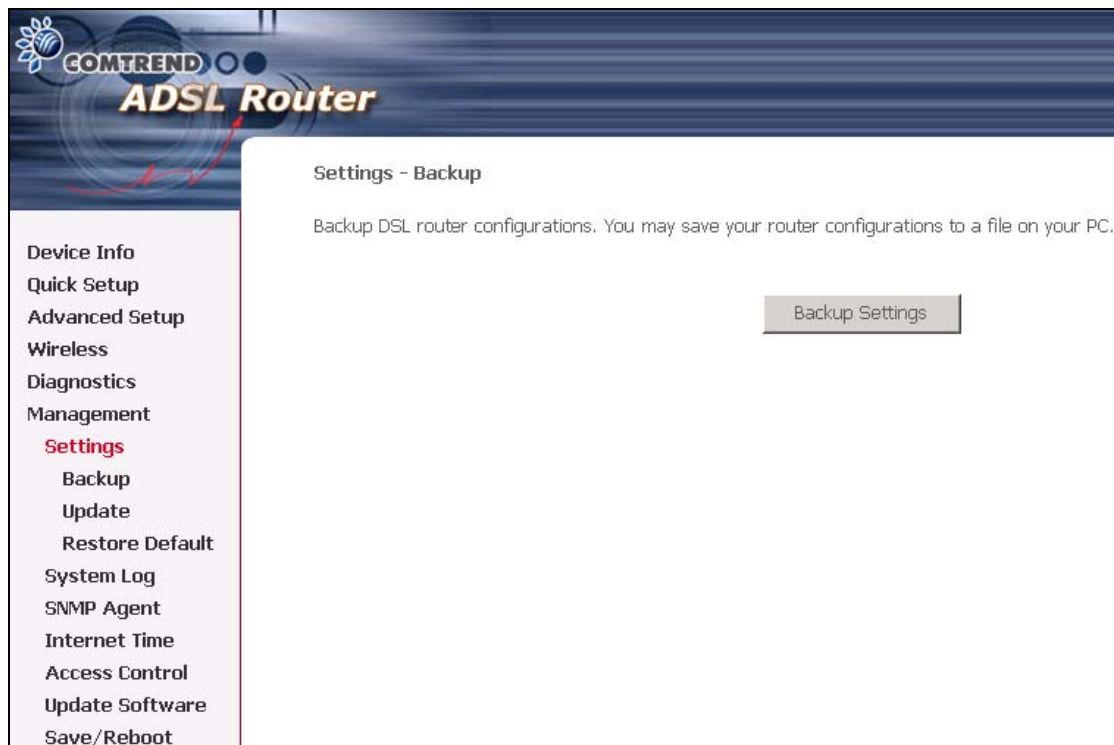
Chapter 9 Management

The Management section of the CT-536+ supports the following maintenance functions and processes:

- Settings
- System log
- SNMP Agent
- Internet Time
- Access Control
- Update software
- Save/Reboot

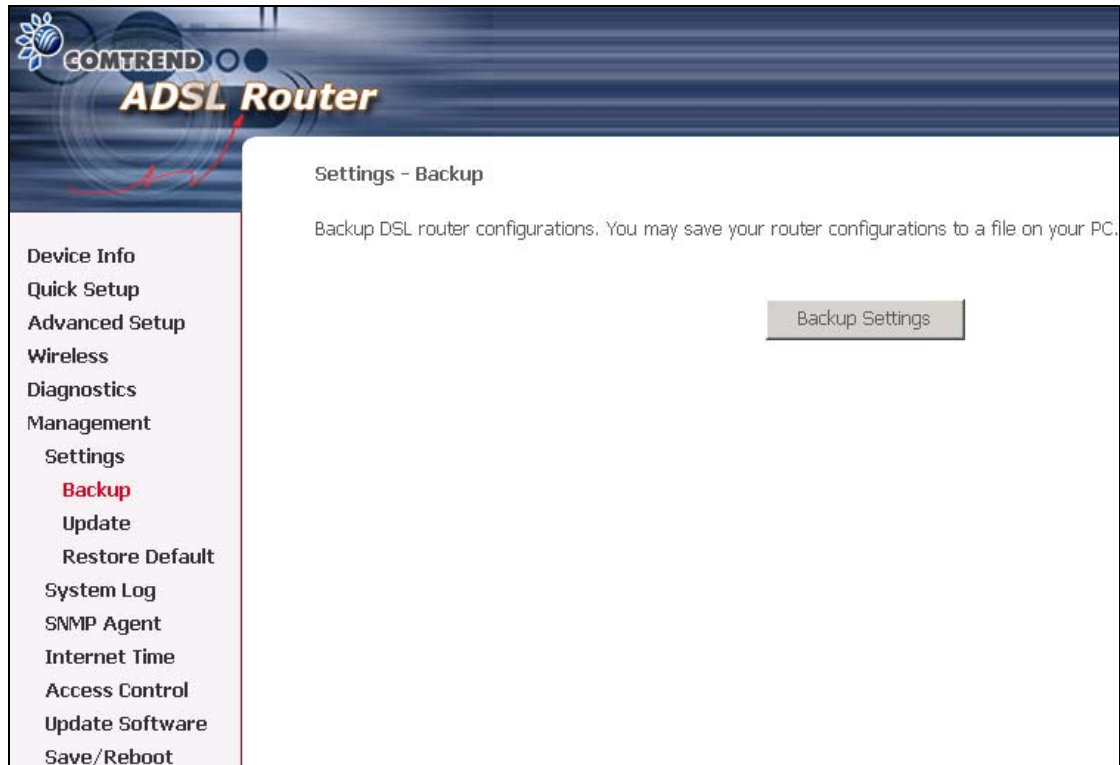
9.1 Settings

The Settings option allows you to back up your settings to a file, retrieve the setting file, and restore the settings.



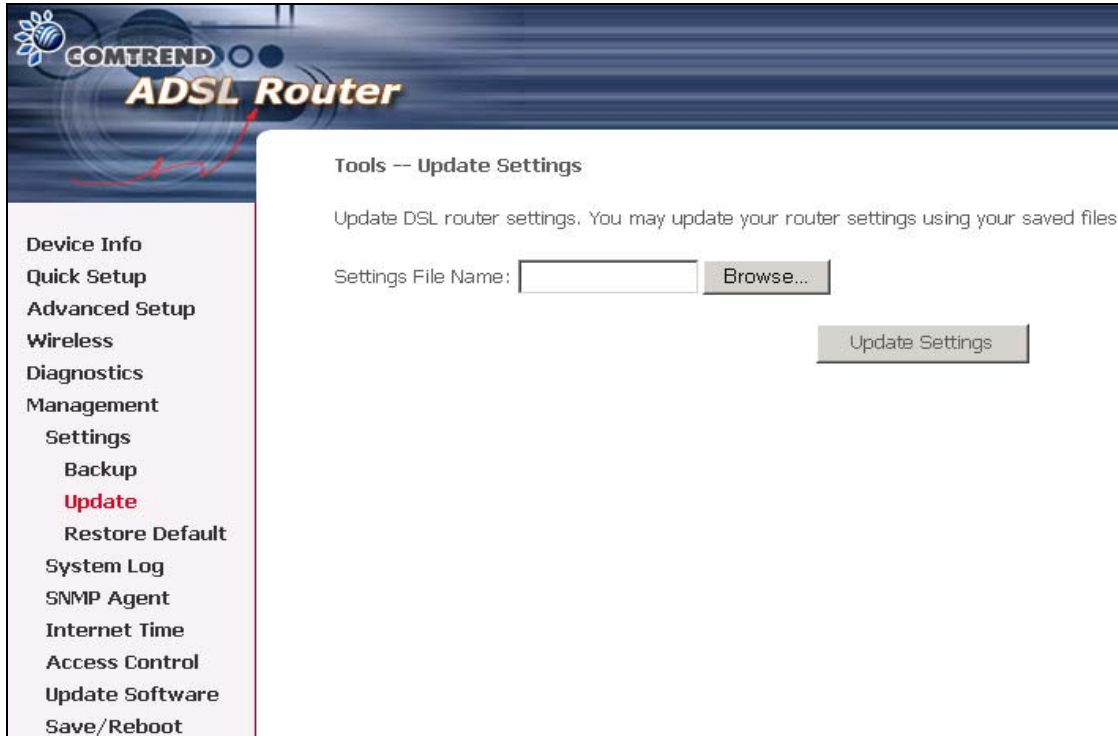
9.1.1 Configuration Backup

The Backup option under Management>Settings save your router configurations to a file on your PC. Click BACKUP Settings in the main window. You will be prompted to define the location of the backup file to save. After choosing the file location, click **Backup Settings**. The file will then be saved to the assigned location.



9.1.2 Tools – Update Settings

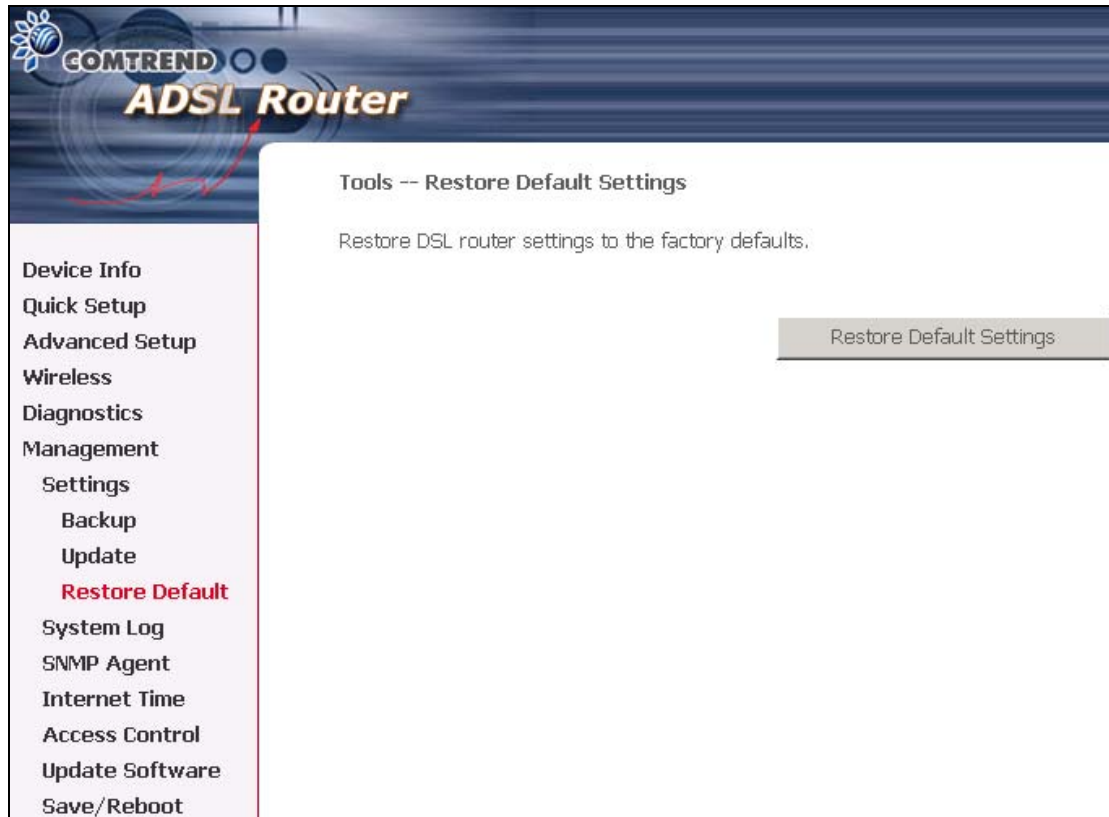
The Update option under Management>Settings update your router settings using your saved files.



The screenshot displays the Comtrend ADSL Router web interface. The header features the Comtrend logo and the text 'ADSL Router'. A left-hand navigation menu lists various settings categories: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, Management, Settings, Backup, Update (highlighted in red), Restore Default, System Log, SNMP Agent, Internet Time, Access Control, Update Software, and Save/Reboot. The main content area is titled 'Tools -- Update Settings' and contains the instruction: 'Update DSL router settings. You may update your router settings using your saved files.' Below this, there is a text input field labeled 'Settings File Name:' followed by a 'Browse...' button. At the bottom right of the main area is an 'Update Settings' button.

9.1.3 Restore Default

Clicking the Restore Default Configuration option in the Restore Settings screen can restore the original factory installed settings.



NOTE: This entry has the same effect as the hardware reset-to-default button. The CT-536+ board hardware and the boot loader support the **reset to default** button. If the reset button is continuously pushed for more than 5 seconds, the boot loader will erase the entire configuration data saved on the flash memory.

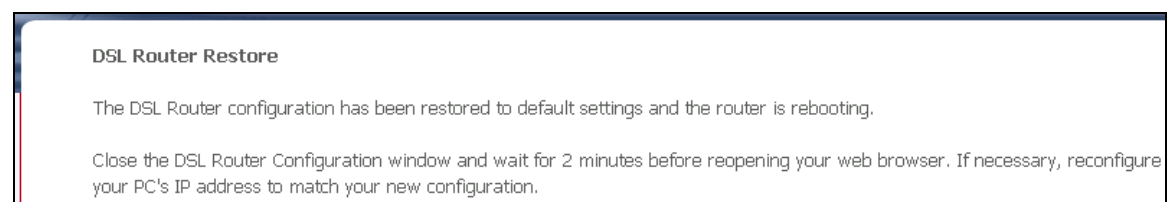
NOTE: Restoring system settings requires a system reboot. This necessitates that the current Web UI session be closed and restarted. Before restarting the connected PC must be configured with a static IP address in the 192.168.1.x subnet in order to configure the CT-536+.

Default settings

The CT-536+ default settings are

- LAN port IP= 192.168.1.1, subnet mask = 255.255.255.0
- Local user name: root
- Password: 12345
- Remote user name: root
- Remote user password: 12345

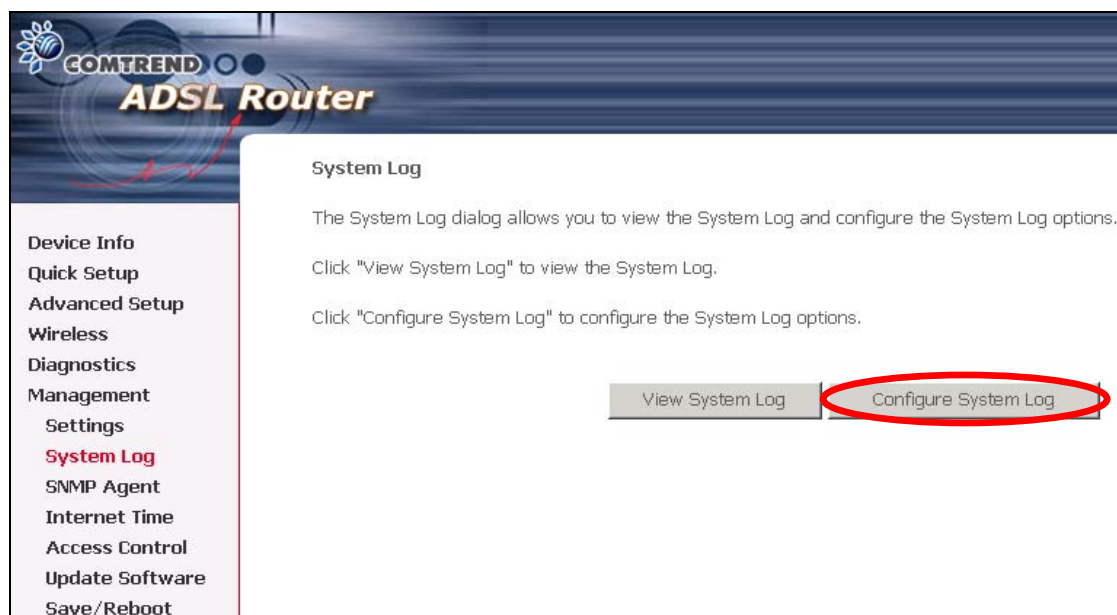
After the Restore Default Configuration button is selected, the following screen appears. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.



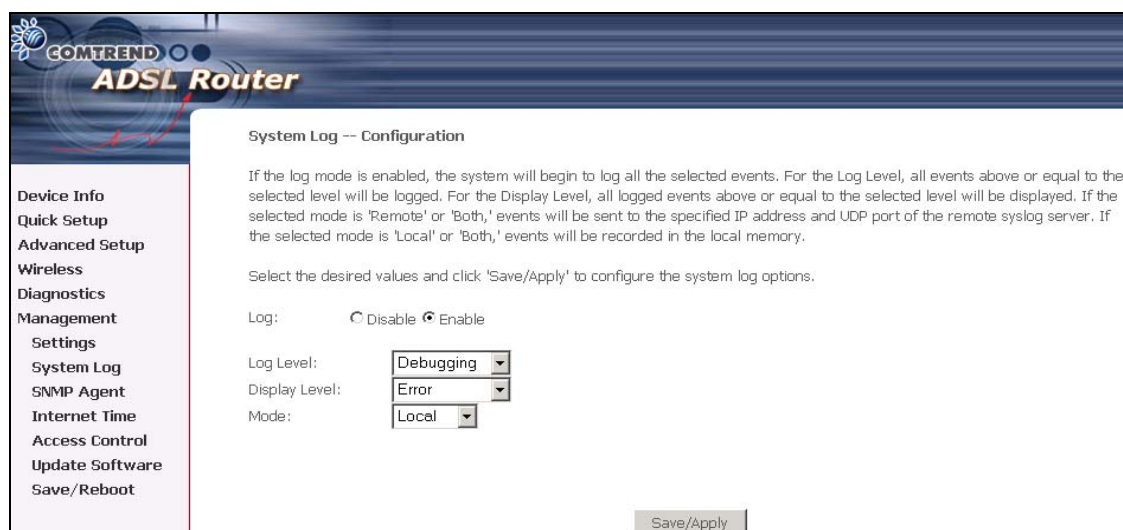
9.2 System Log

The System Log option under Management>Settings allows you to view the system events log, or to configure the System Log options. The default setting of system log is disabled. Follow the steps below to enable and view the system log.

1. Click **Configure System Log** to display the following screen.



2. Select from the desired Log options described in the following table, and then click **SAVE/Apply**.



Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.
Log level	<p>Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-536+ SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are</p> <ul style="list-style-type: none"> ● Emergency = system is unusable ● Alert = action must be taken immediately ● Critical = critical conditions ● Error = Error conditions ● Warning = normal but significant condition ● Notice= normal but insignificant condition ● Informational= provides information for reference ● Debugging = debug-level messages <p>Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.</p>
Display Level	Allows the user to select the logged events and displays on the View System Log page for events of this level and above to the highest Emergency level.
Mode	<p>Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server.</p> <p>When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.</p>

3. Click **View System Log**. The results are displayed as follows.

System Log			
Date/Time	Facility	Severity	Message
Jan 1 00:00:12	syslog	emerg	BCM96345 started: BusyBox v0.60.4 (2004.09.14-06:30+0000)
Jan 1 00:00:17	user	crit	klogd: USB Link UP.
Jan 1 00:00:19	user	crit	klogd: eth0 Link UP.

9.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

The System Log option under Management>Settings allows you to view the system events log, or to configure the System Log options.

Select or enter the desired values and click **Save/Apply** to configure the SNMP options.



- Device Info
- Quick Setup
- Advanced Setup
- Wireless
- Diagnostics
- Management
 - Settings
 - System Log
 - SNMP Agent**
 - Internet Time
 - Access Control
 - Update Software
 - Save/Reboot

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

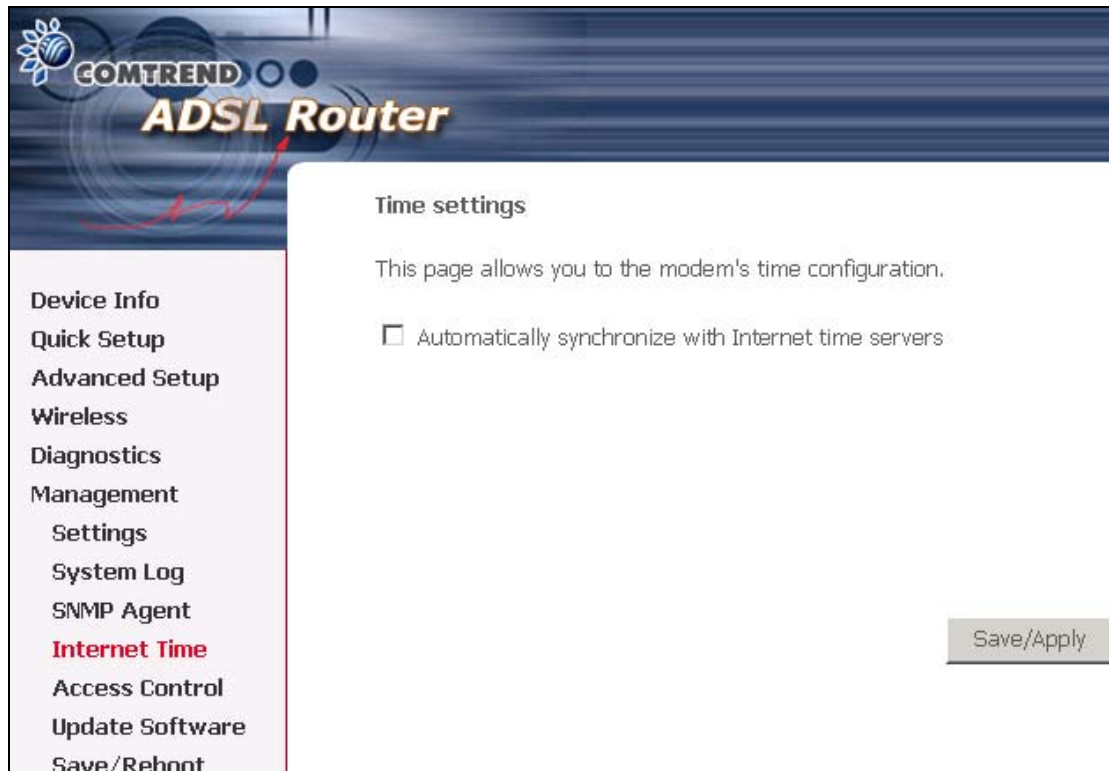
Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent ☒ Disable ☐ Enable

Read Community:	<input type="text" value="public"/>
Set Community:	<input type="text" value="private"/>
System Name:	<input type="text"/>
System Location:	<input type="text" value="unknown"/>
System Contact:	<input type="text" value="unknown"/>
Trap Manager IP:	<input type="text" value="0.0.0.0"/>

9.4 Internet Time

The Internet Time option under Management menu bar configures the Modem's time. To automatically synchronize with Internet Time servers, tick the corresponding box displayed on the screen. Then click **Save/Apply**.



The screenshot displays the web management interface of a COMTREND ADSL Router. The header features the COMTREND logo and the text "ADSL Router". A left-hand navigation menu lists various configuration options: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, Internet Time (highlighted in red), Access Control, Update Software, and Save/Reboot. The main content area is titled "Time settings" and contains the text "This page allows you to the modem's time configuration." Below this text is a checkbox labeled "Automatically synchronize with Internet time servers", which is currently unchecked. A "Save/Apply" button is located in the bottom right corner of the main content area.

9.5 Access Control

The Access Control option under Management menu bar configures the access-related parameters, including three parts: Services, IP Address, and Passwords.

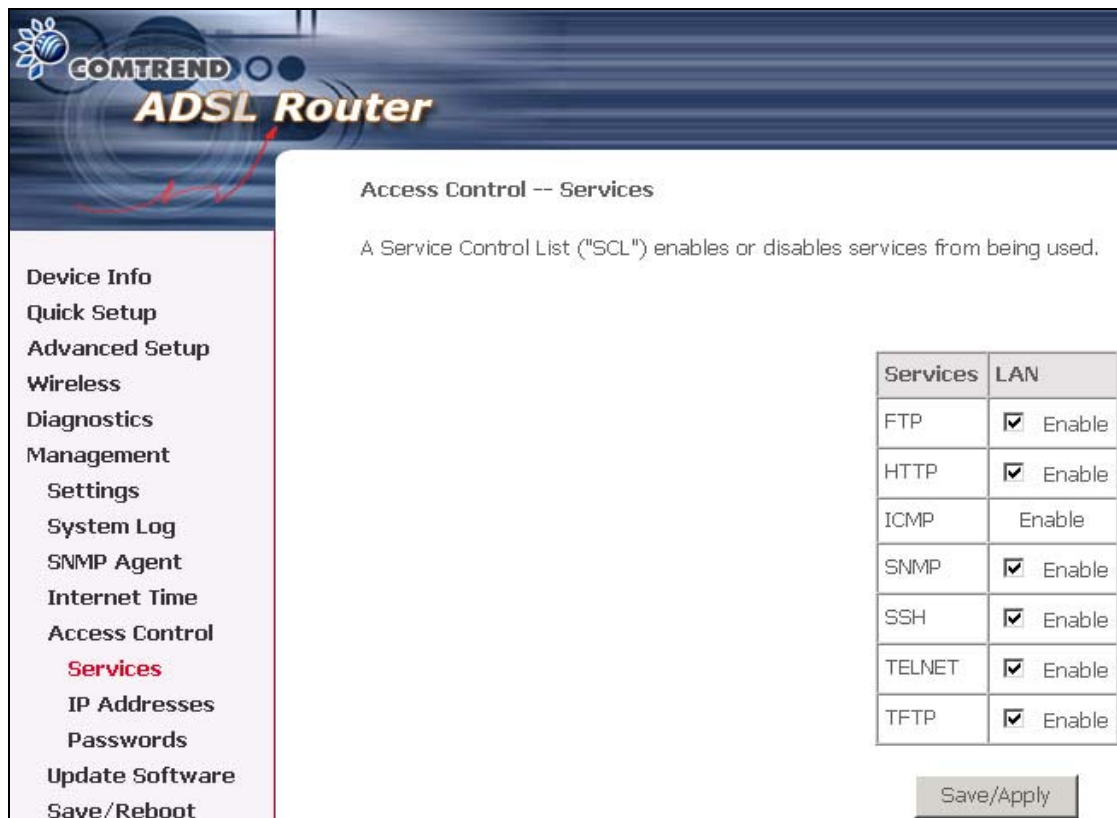
The screenshot displays the Comtrend ADSL Router web interface. The top header features the Comtrend logo and the text "ADSL Router". A left-hand navigation menu lists various configuration options: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, Internet Time, Access Control (highlighted in red), Services, IP Addresses, Passwords, Update Software, and Save/Reboot. The main content area is titled "Access Control -- Services" and includes a descriptive text: "A Service Control List ('SCL') enables or disables services from being used." Below this text is a table with two columns: "Services" and "LAN". The table lists several services with checkboxes and the word "Enable" next to them. At the bottom right of the main content area is a "Save/Apply" button.

Services	LAN
FTP	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable
ICMP	Enable
SNMP	<input checked="" type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable

Save/Apply

9.5.1 Services

The Services option limits or opens the access services over the LAN or WAN. These services are provided FTP, HTTP, ICMP, SNMP, SSH (Security Socket Share), TELNET, and TFTP. Enable the service by checking the item in the corresponding checkbox, and then click **Save/Apply**.



The screenshot shows the COMTREND ADSL Router web interface. The left sidebar contains a menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, Internet Time, Access Control, **Services** (highlighted in red), IP Addresses, Passwords, Update Software, and Save/Reboot. The main content area is titled "Access Control -- Services" and includes a description: "A Service Control List ('SCL') enables or disables services from being used." Below this is a table with two columns: "Services" and "LAN". The table lists seven services: FTP, HTTP, ICMP, SNMP, SSH, TELNET, and TFTP. Each service has a checkbox in the "LAN" column, all of which are checked, and the word "Enable" is displayed next to each checked checkbox. At the bottom right of the main content area is a "Save/Apply" button.

Services	LAN
FTP	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable
ICMP	Enable
SNMP	<input checked="" type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable

Save/Apply

9.5.2 Access IP Addresses

The IP Addresses option limits the access by IP address. If the Access Control Mode is enabled, only the allowed IP addresses can access the router. Before you enable it, configure the IP addresses by clicking the **Add** button. Enter the IP address and click **Apply** to allow the PC with this IP address managing the DSL Router.

The screenshot shows the Comtrend ADSL Router web interface. The left sidebar contains a menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, Internet Time, Access Control, Services, **IP Addresses** (highlighted in red), Passwords, Update Software, and Save/Reboot. The main content area is titled "Management > Access Control > IP Addresses". Below the title, there is a descriptive text: "The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List". Below this text, there is a section for "Access Control Mode" with two radio buttons: "Disable" (selected) and "Enable". Below the radio buttons, there is a table with four columns: "IP Address", "Subnet Mask", "Interface", and "Remove". Below the table, there are two buttons: "Add" and "Remove".

COMTREND
ADSL Router

Management > Access Control > IP Addresses

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode: ☒ Disable ☐ Enable

IP Address	Subnet Mask	Interface	Remove
------------	-------------	-----------	--------

Add Remove

9.5.3 Passwords

The Passwords option configures the access passwords for the router. Access to your DSL router is controlled through three user accounts: root, support, and user.

- "root" has unrestricted access to change and view configuration of your DSL Router.
- "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
- "user" can access the Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click Apply to change or create passwords.

The screenshot shows the web interface of a COMTREND ADSL Router. The left sidebar contains a menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, Internet Time, Access Control, Services, IP Addresses, Passwords (highlighted in red), Update Software, and Save/Reboot. The main content area is titled "Access Control -- Passwords". It contains the following text: "Access to your DSL router is controlled through three user accounts: admin, support, and user." followed by three paragraphs explaining the roles of "admin", "support", and "user". Below this, a note states: "Use the fields below to enter up to 16 characters and click 'Apply' to change or create passwords. Note: Password cannot contain a space." There are four input fields: "Username:" (a dropdown menu), "Old Password:", "New Password:", and "Confirm Password:". A "Save/Apply" button is located at the bottom right of the form area.

COMTREND ADSL Router

Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password:

New Password:

Confirm Password:

Save/Apply

9.6 Update software

The Update Software screen allows you to obtain an updated software image file from your ISP. Manual software upgrades from a locally stored file can be performed using the following screen.



The screenshot shows the 'Tools -- Update Software' page of a Comtrend ADSL Router. On the left is a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, Internet Time, Access Control, Update Software (highlighted in red), and Save/Reboot. The main content area is titled 'Tools -- Update Software' and contains the following instructions:

- Step 1:** Obtain an updated software image file from your ISP.
- Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
- Step 3:** Click the "Update Software" button once to upload the new image file.

A note states: 'NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.' Below the instructions, there is a text input field labeled 'Software File Name:' followed by a 'Browse...' button. At the bottom right of the main content area is a large 'Update Software' button.

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the **Browse** button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

9.7 Save and Reboot

The Save/Reboot options saving the configurations and reboot the router. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.



Appendix A: Firewall

Stateful Packet Inspection

Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

Denial of Service attack

Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack and Tear Drop.

TCP/IP/Port/Interface filtering rules

These rules help in the filtering of traffic at the Network layer i.e. Layer 3.

When a Routing interface is created "Enable Firewall" must be checked.

Navigate to Advanced Setup -> Security -> IP Filtering, web page.

Outgoing IP Filtering: Helps in setting rules to DROP packets from the LAN interface. By default if Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be dropped.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be dropped.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be dropped.

Examples:

1. Filter Name : Out_Filter1
 Protocol : TCP
 Source Address : 192.168.1.45
 Source Subnet Mask : 255.255.255.0
 Source Port : 80
 Dest. Address : N/A
 Dest. Sub. Mask : N/A
 Dest. Port : N/A

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

2. Filter Name : Out_Filter2
 Protocol : UDP
 Source Address : 192.168.1.45
 Source Subnet Mask : 255.255.255.0
 Source Port : 5060:6060
 Dest. Address : 172.16.13.4
 Dest. Sub. Mask : 255.255.255.0
 Dest. Port : 6060:7070

This filter will drop all UDP packets coming from LAN with IP Address/Sub.Mask 192.168.1.45/24 and a source port in the range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port in the range of 6060 to 7070

Incoming IP Filtering:

Helps in setting rules to ACCEPT packets from the WAN interface. By default all incoming IP traffic from WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, particular packet types coming from the WAN can be Accepted.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be accepted.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by the user.

Examples:

1. Filter Name : In_Filter1
Protocol : TCP
Source Address : 210.168.219.45
Source Subnet Mask : 255.255.0.0
Source Port : 80
Dest. Address : N/A
Dest. Sub. Mask : N/A
Dest. Port : N/A

Selected WAN interface: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

2.	Filter Name	: In_Filter2
	Protocol	: UDP
	Source Address	: 210.168.219.45
	Source Subnet Mask	: 255.255.0.0
	Source Port	: 5060:6060
	Dest. Address	: 192.168.1.45
	Dest. Sub. Mask	: 255.255.255.0
	Dest. Port	: 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub.Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC Layer Filtering:

These rules help in the filtering of traffic at the Layer 2. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup -> Security -> MAC Filtering web page.

Global Policy:

When set to Forwarded the default filter behavior is to Forward all MAC layer frames except those explicitly stated in the rules. Setting it to Blocked changes the default filter behavior to Drop all MAC layer frames except those explicitly stated in the rules.

To setup a rule:

Protocol Type: Can be either PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP.

Destination MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular destination address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Source MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular source address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Frame Direction:

LAN <=> WAN --> All Frames coming/going to/from LAN or to/from WAN.

WAN => LAN --> All Frames coming from WAN destined to LAN.

LAN => WAN --> All Frames coming from LAN destined to WAN

User needs to select the interface on which this rule is applied.

Examples:

1.

Global Policy: Forwarded

Protocol Type: PPPoE

Dest. MAC Addr: 00:12:34:56:78:90

Source MAC Addr: N/A

Frame Direction: LAN => WAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule drops all PPPoE frames going from LAN-side to WAN-side with a Dest. MAC Addr. of 00:12:34:56:78:90 irrespective of its Source MAC Addr. on the br_0_34 WAN interface. All other frames on this interface are forwarded.

2.

Global Policy: Blocked

Protocol Type: PPPoE

Dest. MAC Addr: 00:12:34:56:78:90

Source MAC Addr: 00:34:12:78:90:56

Frame Direction: WAN => LAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule forwards all PPPoE frames going from WAN-side to LAN-side with a Dest. MAC Addr. of 00:12:34:56:78:90 and Source MAC Addr. of 00:34:12:78:90:56 on the br_0_34 WAN interface. All other frames on this interface are dropped.

Daytime Parental Control

This feature restricts access of a selected LAN device to an outside Network through the router, as per chosen days of the week and the chosen times.

User Name: Name of the Filter.

Browser's MAC Address: Displays MAC address of the LAN device on which the browser is running.

Other MAC Address: If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

Days of the Week: Days of the week, when the restrictions are applied.

Start Blocking Time: The time when restrictions on the LAN device are put into effect.

End Blocking Time: The time when restrictions on the LAN device are lifted.

Example:

User Name: FilterJohn

Browser's MAC Address: 00:25:46:78:63:21

Days of the Week: Mon, Wed, Fri

Start Blocking Time: 14:00

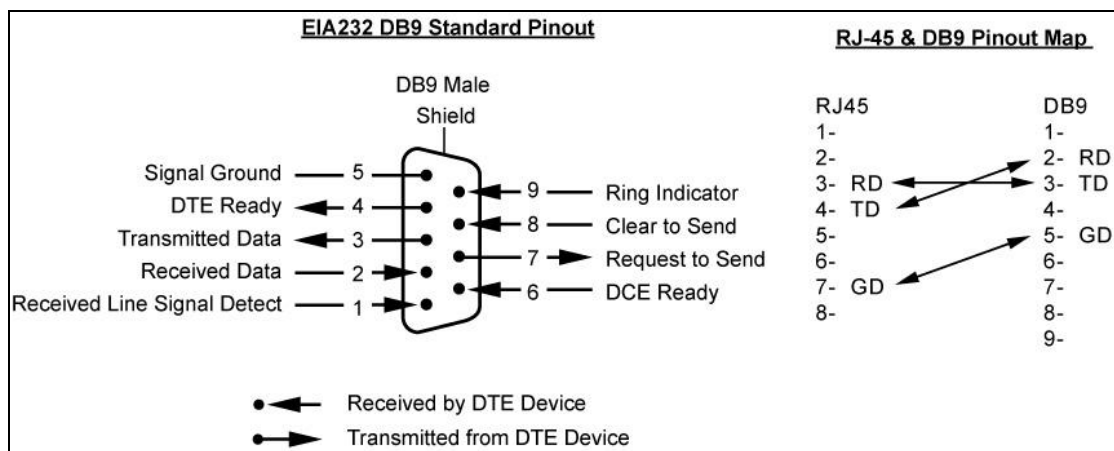
End Blocking Time: 18:00

When this rule i.e. FilterJohn is entered, a LAN device with MAC Address of 00:25:46:78:63:21 will be restricted access to the outside network on Mondays, Wednesdays and Fridays, from 2pm to 6pm. On all other days and time this device will have access to the outside Network.

Appendix B: Pin Assignments

Console (RJ45)

Pin	Definition	Pin	Definition
1	-	6	-
2	-	7	GND
3	RD	8	-
4	TD	9	-
5	-		-



Line port (RJ11)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP
2	-	5	-
3	ADSL_RING	6	-

Pin Assignments of the RJ11 Port

LAN Port (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Pin assignments of the LAN Port

Appendix C: Specifications

Rear Panel

RJ-11 X1 for ADSL, RJ-45 X 4 for LAN, Reset Button X 1, Power Jack X 1, Power switch X 1, Console (RJ45) X 1

ADSL

Standard ANSI T1.413 Issue 2, ITU-T G.992.1, G.992.2 , G.992.3, G.994.1

G.992.5 (ADSL2+) Downstream : 24 Mbps Upstream : 1.3 Mbps

G.992.3 (ADSL2) Downstream : 12 Mbps Upstream : 1.3 Mbps_

G.DMT data rate Downstream: Up to 11 Mbps Upstream: 1 Mbps

G.lite data rate Downstream: 1.5 Mbps Upstream: 512 Kbps

Auto-negotiation rate adaptation

Ethernet

Standard IEEE 802.3, IEEE 802.3u

10/100 BaseT Auto-sense

MDI/MDX support Yes

Wireless

Standard IEEE802.11g, backward compatible with 802.11b

Encryption 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption

Channels 11 Channels (US, Canada)

13 Channels (Europe)

14 Channels (Japan)

Data Rate Up to 54Mbps

WPA/WPA32 Yes

IEEE 802.1x Yes

WMM Yes

ATM Attributes

RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE);

RFC 1577 (IPoA)

Support PVCs 16

AAL type AAL5

ATM service class UBR/CBR/VBR

ATM UNI support UNI3.1/4.0

OAM F4/F5 Yes

Management

SNMP, Telnet, Web-based management, Configuration backup and restoration

Software upgrade via HTTP, TFTP server, or FTP server

Bridge Functions

Transparent bridging and learning	IEEE 802.1d
VLAN support	Yes
Spanning Tree Algorithm	Yes
IGMP Proxy/Snooping	Yes

Routing Functions

Static route, RIP, and RIPv2, NAT/PAT, DHCP Server/DHCP Relay, DNS Proxy, ARP

Security Functions

Authentication protocols PAP, CHAP,
TCP/IP/Port filtering rules, Port triggering/Forwarding, Packet and MAC address filtering, access control, SSH

Application Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc

Power Supply

External power adapter 110 Vac or 220 Vac

Environment Condition

Operating temperature 0 ~ 50 degrees Celsius
Relative humidity 5 ~ 90% (non-condensing)

Dimensions

200 mm (W) x 44 mm (H) x 136.5 mm (D)

Certifications

FCC Part 15 class B, FCC Part 68, CE

Note: Specifications are subject to change without notice

Appendix D: SSH Client

Linux OS comes with ssh client. MicroSoft Windows does not have ssh client but there is a public domain one "putty" that you can download.

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

To access the router using Linux ssh client:

From LAN: Use the router WEB UI to enable SSH access from LAN.

(default is enabled)

type: `ssh -l admin 192.168.1.1`

From WAN: In the router, use WEB UI to enable SSH access from WAN.

type: `ssh -l support router-WAN-ip-address`

To access the router using Windows putty ssh client:

From LAN: Use the router WEB UI to enable SSH access from LAN

(default is enabled)

type: `putty -ssh -l admin 192.168.1.1`

From WAN: In the router, use WEB UI to enable SSH access from WAN.

type: `putty -ssh -l support router-WAN-ip-address`